"Responsabilidad con pensamiento positivo"

UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN

CARRERA: SISTEMAS INFORMÁTICOS

TEMA: AUDITORIA INFORMÁTICA DE SEGUROS DEL PICHINCHA S.A. COMPAÑÍA DE SEGUROS Y REASEGUROS, APLICANDO COBIT 5

AUTOR: LUIS PATRICIO AUQUILLA CHAVEZ

TUTOR: RENE ALBERTO CAÑETE, PhD

2014

DEDICATORIA

Esta tesis se la dedico a mi Dios quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mi familia quienes por ellos soy lo que soy.

Para mis padres por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

Mil palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en los momentos difíciles.

A mis hermanos por estar siempre presentes, acompañándome para poderme realizar. A mis sobrinas que son una motivación, inspiración y felicidad.

A todos, espero no defraudarlos y contar siempre con su valioso apoyo, sincero e incondicional.

AGRADECIMIENTO

Primero y antes que nada, dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente

Agradecer hoy y siempre a mi familia por el esfuerzo realizado por ellos. El apoyo en mis estudios, de ser así no hubiese sido posible. A mis padres y demás familiares ya que me brindan el apoyo, la alegría y me dan la fortaleza necesaria para seguir adelante.

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORÍA DE TESIS

La abajo firmante, en calidad de estudiante de la Carrera de Sistemas Informáticos declaro que los contenidos de este Trabajo de Graduación, requisito previo a la obtención del Grado de Ingeniero en Sistemas Informáticos, son absolutamente originales, auténticos y de exclusiva responsabilidad legal y académica del autor.

Quito, octubre del 2014

Luis Patricio Auquilla Chavez

CC: 171641633-2

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Graduación certifico:

Que el Trabajo de Graduación "AUDITORIA INFORMÁTICA DE SEGUROS DEL PICHINCHA S.A. COMPAÑÍA DE SEGUROS Y REASEGUROS, APLICANDO COBIT 5", presentado por Luis Patricio Auquilla Chavez, estudiante de la carrera de Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito, octubre 2014

TUTOR

Rene Alberto Cañete, PhD

RESUMEN

El presente proyecto de titulación está compuesto de cuatro capítulos y anexos, que tienen como principal objetivo, presentar los resultados de la auditoria informática realizada a una institución aseguradora, utilizando las directrices de auditoria de COBIT 5.

En el Capítulo I se detallan los antecedentes investigativos y fundamentación científico y técnica debidamente justificados, además se exponen algunos conceptos y parámetros que definen a la Auditoria Informática, relacionados con el ambiente de control, sus procesos y los controles de TI.

En el Capítulo II se detalla la metodología Cobit 5(Control Objectives for Information and Related Technology), estándar generalmente aceptado para buenas prácticas en seguridad tecnológica y en administración y control de la tecnología de la información. En este Capítulo se detalla el tipo de investigación a realizarse, el cómo y con qué instrumento se llevara a cabo la investigación para una determinada población y muestra.

En el Capítulo III se presenta la ejecución de la auditoria informática, el análisis de riesgos de los hallazgos de vulnerabilidades y la elaboración del informe final de auditoria con las recomendaciones emitidas en la institución aseguradora, para mitigar los riesgos identificados en la institución.

Finalmente en el último capítulo se presentan las conclusiones y recomendaciones del presente proyecto

ABSTRACT

This graduation project is composed of four chapters and appendices, which are aimed to present the results of the computer audit on an insurance institution, using guidelines audit COBIT 5.

In Chapter I the background research and scientific and technical detailing duly substantiated grounds, plus some concepts and parameters that define the Computer Audit exposed, related to the control environment, processes and IT controls.

In Chapter II the methodology Cobit 5 (Control Objectives for Information and Related Technology), generally accepted standard for good practice in safety technology and management and control of information technology is datalla. In this chapter the type of research to be carried out is detailed, and the like that will be held instrument for a particular research population and sample.

The execution of computer audit, the risk analysis of the findings of vulnerabilities and the preparation of the final audit report with recommendations issued by the insurance institution is presented in Chapter III, to mitigate the risks identified in the institution.

Finally in the last chapter the conclusions and recommendations of this project are presented.

INDICE GENERAL

DEDICATORIA ii
AGRADECIMIENTO iii
AUTORÍA DE TESIS iv
APROBACIÓN DEL TUTOR v
RESUMEN vi
ABSTRACT vii
INDICE GENERAL viii
ÍNDICE DE TABLAS xi
ÍNDICE DE FIGURAS xiii
INTRODUCCIÓN I
Introducción General I
Antecedentes II
Descripción del problema a resolver IV
Objeto de estudio IV
Campo de investigación IV
Objetivo General IV
Objetivos Específicos IV
Ideas a Defender V
CAPITULO I 1
1. MARCO TEORICO 1
1.1. Antecedentes Investigativos 1
1.2. Fundamentación Científico – Técnica 2
1.2.1. Auditoría 2
1.2.1.1. Clasificación de las auditorias 2
1.2.2. Auditoría Informática 3
1.2.2.1 Objetivos de la Auditoria Informática 3
1.2.2.2 Bases de la Auditoria Informática 3
1.2.2.3 Tipos y Clases de Auditoria Informática 4
1.2.3. COBIT 5
1.2.4. COBIT 5 6
1.2.5 COSO 12
1.2.6 ITIL 14

CAPÍTULO II 17
2. METODOLOGÍA Y DIAGNÓSTICO DE LA INVESTIGACIÓN 17
2.1. Fuentes de información 17
2.2. Metodología de la investigación 17
2.3. Técnicas e instrumentos de recolección de datos 18
2.4. Plan de Muestreo 18
2.5. Trabajo de campo 19
2.6. Procesamiento de la información 20
2.7. Análisis e interpretación de resultados. 28
2.8. Problemas y especificación de requerimientos. 29
2.9. Estudio de Factibilidad 29
2.9.1. Estudio de Factibilidad Operativa 29
2.9.1.1 Resistencia al cambio 29
2.9.1.2. Viabilidad de la Implementación 30
2.9.1.3. Impacto Tecnológico 30
2.9.2. Estudio de Factibilidad Tecnológica 30
2.9.2.1. Plataforma, Sistemas, Interconectividad. 30
2.9.3. Estudio de Factibilidad Económica 36
2.9.3.1. Costo de la Auditoria 36
2.9.3.2. Recurso Humano 36
2.9.3.3 Recursos Materiales 36
2.9.3.4. Recursos Varios 36
2.9.3.5. Tabla Resumen 37
CAPÍTULO III 38
3. PROPUESTA 38
3.1. Antecedentes de la propuesta 38
3.2. Justificación 39
3.3. Objetivos de la propuesta 40
3.3.1. General 40
3.3.2. Específicos 40
3.4. Desarrollo de la Propuesta. 40
3.4.1. Estudio Preliminar del Entorno a Auditar 40
3.4.2. Estudio del Departamento de Tecnología de la Información 49
3.4.3. Planeación de la auditoria informática a Seguros del Pichincha 55

3.4.3.1. Planeación Previa 55
3.4.3.2. Estudio preliminar 56
3.4.3.3. Desarrollo de la estrategia de la auditoria 56
3.4.3.4 Descripción del Mapa de Relación COBIT – SEGUROS DEL PICHINCHA 65
3.4.3.5 Descripción de las Matrices 66
3.4.3.6 Determinación de Resultados y Productos de la Auditoría 71
3.4.3.7 Recursos para la auditoría 73
3.4.3.8 Programa de auditoría 76
3.4.3.9 Cronograma de actividades para la Auditoría 77
3.5 Informe de Auditoría 78
3.5.1 Carta de Presentación de la Auditoría Informática 78
Análisis de la Seguridad de la información de Seguros del Pichincha 82
CONCLUSIONES 96
RECOMENDACIONES 97
BIBLIOGRAFIA 98
ANEXOS 100
Anexo 1: Tabulación de encuestas A para la empresa Seguros del Pichincha s.a 100
Anexo 2: Tabulación de encuesta B para la empresa Seguros del Pichincha s.a 110
Anexo 3: Tabulación de encuesta C para la empresa Seguros del Pichincha s.a 120
Anexo 4: Estándares de Software y Hardware 125
Anexo 5: Planos y Matrices COBIT Desarrollados durante la ejecución de la Auditoria de Seguros del Pichincha 129

ÍNDICE DE TABLAS

Tabla 2.1. Características de los Sistemas Operativos 31
Tabla 2.2. Características de los Sistemas Operativos en los Servidores 32
Tabla 2.3. Características del Paquete de Programas Informáticos 32
Tabla 2.4. Características de los Programas Internos. 33
Tabla 2.5. Costo de desarrollo de la Auditoria Recursos humanos 36
Tabla 2.6. Costo de desarrollo de la Auditoria Recursos Materiales 36
Tabla 2.7. Costo de desarrollo de la Auditoria Recursos Varios 36
Tabla 2.8. Costo total del desarrollo de la Auditoria 37
Tabla 3.1. Objetivos del Departamento de TI de Seguros del Pichincha 50
Tabla 3.2. Matriz Foda del Departamento de TI. SDP 52
Tabla 3.3. Recursos Humanos de TI 52
Tabla 3.4. Recursos Humanos de DTI-Regionales 53
Tabla 3.5. Presupuesto Referencial 55
Tabla 3.6. Procesos y Objetivos de Gobierno COBIT. 58
Tabla 3.7. Metas Generales de TI de Seguros del Pichincha 59
Tabla 3.8. Metas de TI – COBIT (COBIT 5, 2012) 59
Tabla 3.9. Métricas y Mediciones de la Auditoria Informática a Seguros del Pichincha 60
Tabla 3.10. Componentes del Mapa de Relación COBIT-Seguros del Pichincha 60
Tabla 3.11.Equivalencias del Impacto 62
Tabla 3.12. Parámetros del indicador de Madurez 63
Tabla 3.13. Parámetros del Indicador de Desempeño 64
Tabla 3.14. Parámetros del Indicador de Cumplimiento de Objetivos 64
Tabla 3.15. Parámetros del Indicador de Impacto 65
Tabla 3.16. Modelo Genérico de Madurez – COBIT.(COBIT,2012) 67
Tabla 3.17. Equivalencias de Desempeño 68
Tabla 3.18. Interpretación de los Impactos de acuerdo a COSO 69
Tabla 3.19. Equivalencias del Impacto 70
Tabla 3.20. Equivalencias Cuantitativas de la Importancia 71
Tabla 3.21. Selección de la muestra. 76
Tabla 3.22. Programa de Auditoria 77
Tabla 3.23 Cronograma de Auditoria 78
Tabla 3.24. Catalogo de Servicios 81
Tabla 3.25. Dominio para pruebas de Hacking Etico Externo 83
Tabla 3.26. Vulnerabilidades Seguros del Pichincha para pruebas externas 84
Tabla 3.27. Objetivos de análisis para pruebas internas de Hacking Etico 85
Tabla 3.28. Objetivo de análisis para pruebas internas de Hacking Etico 91
Tabla 3.29. Informacion recolectada en pruebas de ingeniería social 92
Tabla 3.30. Recomendaciones Hacking Etico 93
Tabla A5.1. Plano de enlace de las metas de la institución, metas TI y Criterios de Informacion . 129
Tabla A5.2. Plano de enlace de las metas TI, Procesos COBIT y Criterios de información 130
Tabla A5.3. Plano de enlace de las metas relacionados con las TI y los Procesos relacionados con TI 131

Tabla A5.4. Plano de enlace de las metas relacionados con las TI y los procesos relacionados con TI 132
Tabla A5.5. Plano de enlace de las metas corporativas de COBIT 5 y las metas relacionadas con TI 138
Tabla A5.6. Plano de responsabilidades de Procesos COBIT..... 139
Tabla A5.7. Matriz de Grados de Procesos – Seguros del Pichincha..... 140
Tabla A5.8. Matriz de Nivel de usuarios – Seguros del Pichincha..... 141
Tabla A5.9. Matriz de Cumplimiento de Objetivos de Gobierno 142
Tabla A5.10. Matriz de Impacto de Procesos frente a los criterios de Informacion de COBIT..... 143

ÍNDICE DE FIGURAS

Figura 1. Organigrama Seguros del Pichincha. III
Figura 1.1. A.I. como intersección de otras disciplinas. 4
Figura 1.2. Principios de COBIT 5 7
Figura 1.3. Habilitadores de COBIT 5 8
Figura 1.4. Marco de Trabajo Completo de COBIT. 10
Figura 1.5. Familia de Productos COBIT. 11
Figura 1.6. Categorías de Catalizadores COBIT. 11
Figura 1.7. Componentes de COSO-ERM. 13
Figura 1.8. Flujos de Información ERM. 14
Figura 1.9. Biblioteca de Infraestructura de la Información 16
Figura 2.1. Pirámide de Procesos 19
Figura 2.2. Niveles de descripción de requerimientos utilizados en las diferentes fases del proceso de ingeniería de requerimientos. 29
Figura 2.3. Diagrama de Servidores 34
Figura 2.4.Topologia de Red Seguros del Pichincha 35
Figura 3.1. Cadena de Valor de Seguros del Pichincha 51
Figura 3.2. Dimensiones del Estado del Proceso 61
Figura 3.3. Productos de Auditoria Informática para Seguros del Pichincha 72
Figura 3.4. Resultados de Auditoria Informática para Seguros del Pichincha 73
Figura 3.5. Selección de la Muestra de Auditados 75
Figura 3.6. Equipos externos afectados por vulnerabilidades 83
Figura 3.7. Plan para definir las políticas y procedimientos de Seguridad de la Información 94
Figura 3.8. Plan para creación del área de Seguridad de la Información 95
Figura A4.1. Estándares de Software 125
Figura A4.2. Estándares de Hardware – Servidor tipo Blade 126
Figura A4.3. Estándares de Hardware-Computadores de Escritorio 126
Figura A4.4. Estándares de Hardware-Computadores Portátiles 127
Figura A4.5. Estándares de Hardware – Impresoras 127
Figura A4.6. Estándares de Hardware - Teléfonos 128

INTRODUCCIÓN

Introducción General

En el Ecuador existen compañías aseguradoras divididas en los siguientes sectores: seguros generales 11 compañías, seguros generales y de vida 22 compañías y netamente seguros de vida 7 compañías. La competencia de las empresas de seguros en el país crece, ante lo cual se realizan alianzas para captar mayores clientes y poder fortalecer las posiciones situacionales de las organizaciones.

Seguros del Pichincha es una organización que cuenta con más de 19 años de experiencia en asegurar lo más trascendental que tiene las personas su vida. Es una empresa líder en el mercado asegurando personas

La auditoría está alcanzando un rol cada vez más importante en diferentes áreas como son de desempeño, privacidad y seguridad. Satisfacer las regulaciones de cumplimiento y mitigar los riesgos relacionados con las amenazas internas son algunos de los retos de seguridad más significativos a los que se afrontan las empresas.

La auditoría informática se encarga de verificar el correcto funcionamiento de los equipos de TI así como analizar el software legal e ilegal que posee la aseguradora.

El desarrollo de las metodologías en las auditorias ayuda a incorporar un conjunto de procedimientos. La Metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno.

COBIT es una herramienta desarrollada para ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías, las buenas prácticas de COBIT están enfocadas en el ambiente de control óptimo que debe tener una empresa para de esta manera lograr una alineación efectiva entre TI y los objetivos de negocio. (COBIT 5, 2012)

Antecedentes

SEGUROS DEL PICHINCHA S.A. COMPAÑÍA DE SEGUROS Y REASEGUROS., es una empresa binacional, de capital Colombo – Ecuatoriano, constituida mediante escritura pública el 24 de enero de 1995, aprobada por la Superintendencia de Bancos según resolución 95 – 035 – s del 03 de febrero de 1995 e inscrita en el Registro Mercantil el 17 de febrero del mismo año. Su casa matriz está ubicada en la Av. González Suarez N32-346 y Coruña en la ciudad de Quito, República del Ecuador.

La compañía tiene como objetivo desarrollar actividades y negocios de seguros y reaseguros permitidos por la Ley de la materia, así como realizar todo acto o contrato lícito para el cumplimiento de sus fines de conformidad con las normas jurídicas vigentes

SEGUROS DEL PICHINCHA S.A. opera en todos los ramos o modalidades de seguros de vida y generales que se encuentran vigentes en el mercado, aprobados por la Superintendencia de Bancos.
La empresa decidió trabajar con mayor énfasis en los ramos de seguros personales en los que brinda mayor servicio y sobre todo en protección económica familiar.

SEGUROS DEL PICHINCHA S.A. su lema "una familia para la familia se dedica a Seguros de Vida individuales y colectivos''.

SEGUROS DEL PICHINCHA S.A. es una de las principales aseguradoras generales y de vida, cuenta con el apoyo de la mayor institución financiera en el país (GRUPO PICHINCHA), que le permite acceder a coberturas colectivas y la creación de alianzas con otras instituciones financieras.
La misión de Seguros del Pichincha es desarrollar la actividad de seguros optimizando la rentabilidad a largo plazo con un servicio sobresaliente y dentro de los más altos principios de ética profesional.
La visión de Seguros del Pichincha es ser líderes en el mercado asegurador de personas, entregando a sus clientes servicios con valor agregado de alto impacto social, con profesionales éticos, comprometidos y en constante desarrollo, generando sólidos resultados que aporten al crecimiento económico y social del país.

El organigrama de Seguros del Pichincha es:

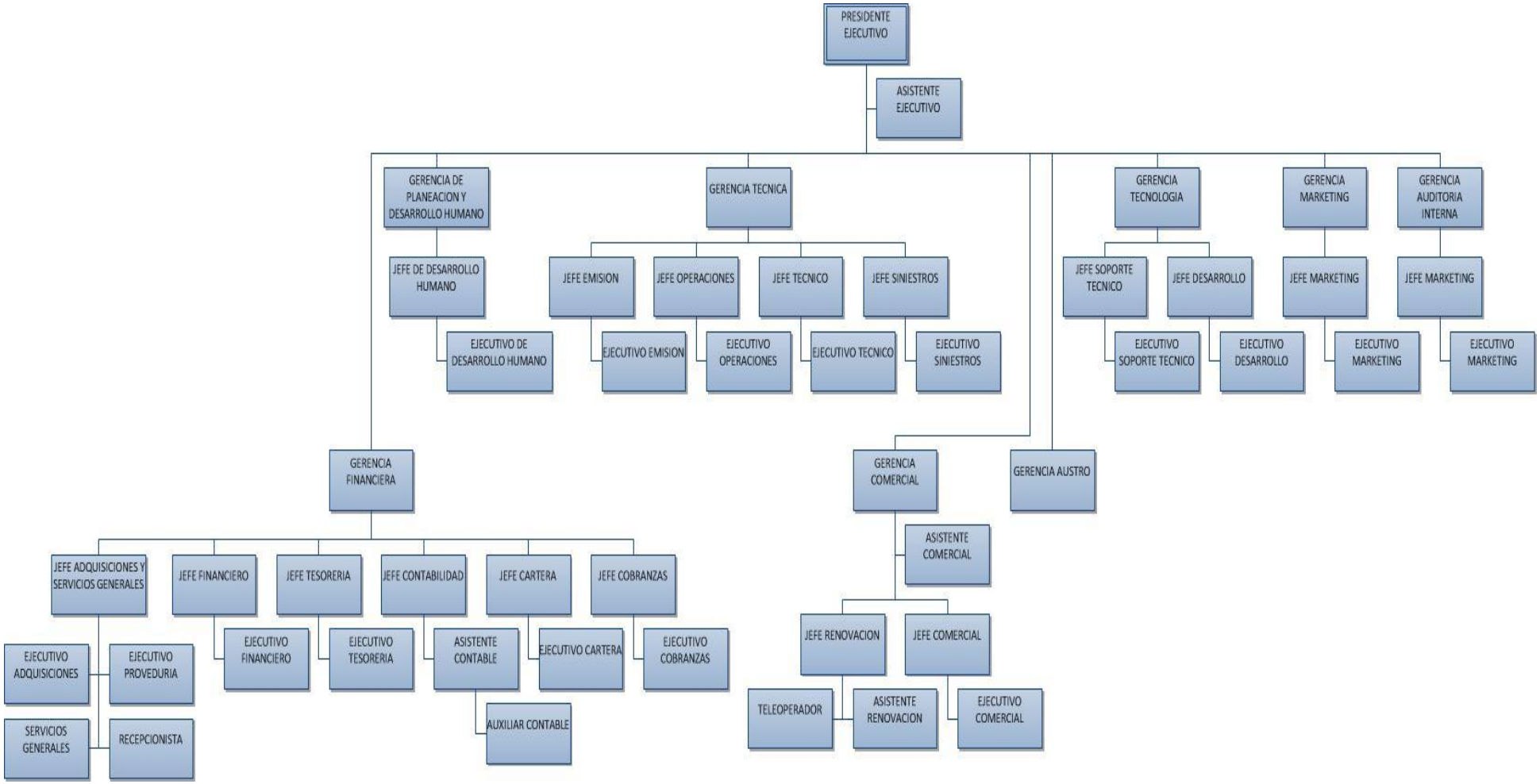


Figura 1. Organigrama de Seguros del Pichincha
Elaborado por el Autor

Descripción del problema a resolver

El departamento tecnológico de Seguros del Pichincha S.A. ha delatado fallas en sus Sistemas de Información, en los procedimientos de seguridad en la información de sus sistemas informáticos, los que ocasionan retrasos en las operaciones de la empresa, por lo cual necesitan verificar las vulnerabilidades y oportunidades de mejora en sus sistemas, ya que pérdidas de tiempo y dinero se ven constantemente relacionadas con problemas con los sistemas.

Objeto de estudio

Aplicación de la Ingeniería Informática para la revisión práctica de los recursos informáticos con que cuentan las empresas aseguradoras.

Campo de investigación

Análisis, de la verificación y de exposición de debilidades y disfunciones de los sistemas de información de la sociedad anónima Seguros del Pichincha.

Objetivo General

Realizar una Auditoría Informática del Sistema de Información de SEGUROS DEL PICHINCHA S.A. COMPAÑIA DE SEGUROS Y REASEGUROS, utilizando el estándar internacional COBIT 5, a fin de identificar debilidades y emitir informes que permitan la toma de decisiones por parte de la gerencia.

Objetivos Específicos

Realizar una investigación bibliográfica que permita conocer las principales tendencias en cuanto a procedimientos y estándares internacionales de Tecnologías de la Información, los mismos que servirán como fundamento teórico del proyecto.

Diagnosticar y Analizar la información obtenida de la situación actual en relación a la recurrencia de los incidentes, mediante la aplicación del método científico.

Realizar el procedimiento de auditoria aplicando el estándar COBIT 5 en la evaluación y auditoria de sistemas en Seguros del Pichincha s.a.

Conocer, categorizar, priorizar y documentar los problemas, exigidos por el estándar internacional adoptada para el diseño del presente proyecto, que permita la evaluación de los expertos.

Ideas a Defender

Mediante la elaboración de una Auditoria Informática, utilizando el estándar internacional COBIT 5, se identificara las debilidades en la seguridad en los sistemas de información y emitir informes que permitan la toma de decisiones por parte de la gerencia.

CAPITULO I

1. MARCO TEORICO

1.1. Antecedentes Investigativos

Se ha determinado que la Compañía de Seguros del Pichincha s.a., ubicada su matriz en la ciudad de Quito, no ha planificado, ni ejecutado ningún proyecto de investigación sobre el problema de estudio de una Auditoria Informática, este juicio permite asegurar que este trabajo investigativo planteado tiene un enfoque de originalidad y sus resultados permitirán poner las bases para un futuro exitoso de la compañía.

SEGUROS DEL PICHINCHA S.A. opera en todos los ramos o modalidades de seguros de vida y generales que se encuentran vigentes en el mercado, aprobadas por la Superintendencia de Bancos.
La empresa decidio trabajar con mayor enfasis en los ramos de seguros personales en los que brinda mayor servicio y sobre todo proteccion familiar.

En la actualidad varias empresas aseguradoras se encuentran realizando su labor de una forma que para los estandares actuales de tecnología pueden calificarse como rudimentarias.Es así que para el manejo de la información au no se utiliza una fuente fidedigna que cumpla con todos los estándares internacionales que se acople a las necesidades de su actividad, lo cual con lleva a un bajo desempeño institucional y una falta de disponibilidad de la información.

En el presente, la aseguradora es cada vez más dependiente de sus redes informáticas y un problema que les afecte por mínimo que sea puede llegar a comprometer la continuidad de las operaciones y transacciones realizadas. Han surgido muchos problemas relacionados con el uso de computadoras , amenazas que afectan negativamente tanto a individuos a como la empresa. Se accede de manera indebida, sin autorización , a un sistema de tratamiento de información, con el fin de obtener una satisfacion de carácter intelectual o económico por el desciframiento de los codigos de acceso.

1.2. Fundamentación Científico – Técnica

1.2.1. Auditoría

A la auditoría se la vincula como una rendición de cuentas con el fin de descubrir errores pero la explicación de auditoria va más lejos.

> Sostiene que la auditoria es un proceso necesario para las organizaciones con el fin de asegurar que todos sus activos sean protegidos en forma adecuada. En donde, la alta dirección espera que de estos procesos de auditoria surjan recomendaciones necesarias para la mejora continua de las funciones de la organización (Hernández Hernández Enrique, 1997:16)

1.2.1.1. Clasificación de las auditorias

Yanez e Ibsen (2011) señalan que existen varias formas de clasificar a la auditoría, simplemente si se piensa en las áreas de especialización, éstas darían una clasificación extensa y válida. Sin embrago, en esta ocasión se mencionarán dos tipos, las cuales pueden aportar elementos de interés en su posterior estudio.

La auditoría de gestión, está orientada a la evaluación de aspectos relacionados con la eficiencia y productividad de las operaciones de una organización. Este tipo de auditoría, al igual que la integral que se menciona a continuación, puede ser desempeñada tanto por auditores externos como internos.

Constituye objeto de la auditoría de gestión, el proceso administrativo, las actividades de apoyo y operativas; la eficiencia, efectividad y economía en el empleo de los recursos humanos, financieros, ambientales, tecnológicos y de tiempo; y el cumplimiento de las atribuciones institucionales.

La auditoría integral, se realiza con el fin de evaluar en su totalidad los objetivos que existen en una organización, es decir, los relacionados con información financiera, salvaguardar los activos, eficiencia y normativa, entre otros. Este tipo de auditorías también pueden ser realizadas tanto por auditores externos como internos.

1.2.2. Auditoría Informática

La auditoría informática consiste en el examen crítico y sistemático de las políticas, normas, prácticas y procedimientos para dictaminar respecto a la economía, eficiencia y eficacia de los usos de los recursos de TI, efectividad del sistema de control interno asociado a las TI, confiabilidad y validez de la información.

> La auditoría se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de la información en la organización, se lleven a cabo de una manera oportuna y eficiente" (Piattini Velthuis & del Peso Navarro,2000:15)

1.2.2.1 Objetivos de la Auditoria Informática

> Piattini sostiene que la auditoria informática confirma la consecución de los objetivos tradicionales de la auditoria: objetivos de protección de activos e integridad de datos; y objetivos de gestión, que abarcan no solamente los de protección de activos, sino también los de eficacia y eficiencia. (Piattini, Del Peso, 2003). Caridad Simon en sus apuntes de Auditoría Informática (2006, p.15) cita a Ron Weber (1982) quien separa los objetivos de la AI en cuatro grupos: objetivos de salvaguarda de bienes; objetivos de integridad de datos; objetivos de efectividad del sistema y objetivos de eficiencia del sistema. (Caridad Simon, 2006)

1.2.2.2 Bases de la Auditoria Informática

Serafín Caridad Simón (2006), en su obra Auditoría Informática, considera a la Auditoría Informática (AI) como la intersección de cuatro disciplinas: Auditoría Tradicional, Ciencias del Comportamiento, Gestión de Sistemas de Información e Informática. Eso se muestra en la Figura 1.1

Figura 1.1. A.I. como intersección de otras disciplinas.
Basado en Caridad Simon, (2006,p.18).

1.2.2.3 Tipos y Clases de Auditoria Informática

Dentro de las áreas generales, es posible establecer las siguientes divisiones:

Auditoria Informática de Explotación

Auditoria Informática de Sistemas

Auditoria Informática de Comunicaciones y Redes

Auditoria Informática de Desarrollo de proyectos

Auditoria Informática de Seguridad

Auditoria Informática de Explotación: La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc.

Auditoria Informática de Sistemas: Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas.

Sistemas Operativos

Software Básico

Software de Teleproceso (Tiempo Real)

Tunning

Optimización de los sistemas y subsistemas

Administración de Base de Datos

Investigación y Desarrollo

Auditoria Informática de Comunicaciones y Redes: Revisión de la topología de Red y determinación de posibles mejoras, análisis de caudales y grados de utilización

Auditoria Informática de Desarrollo de proyectos: Revisión del proceso completo de desarrollo de proyectos por parte de la empresa auditada.

El análisis se basa en cuatro aspectos fundamentales:

Revisión de las metodologías utilizadas

Control Interno de las Aplicaciones

Satisfacción de usuarios

Control de Procesos y Ejecuciones de Programas Críticos

Auditoria Informática de Seguridad: La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La Seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Igualmente, a este ámbito pertenece la política de Seguros .La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información. (Escuela Superior de Tlahuelipan, 2011)

1.2.3. COBIT

Isaca (2012) considera que COBIT tiene su base en los objetivos de control ISACF, actualmente conocida COMDISACA (Information System Audit and Control Association), de acuerdo a estándares internacionales, este modelo de referencia tiene la facilidad de adaptarse a cualquier tipo de negocio y los objetivos de control que se haya definido en el modelo, pueden ser aplicados independientemente del ambiente, plataformas y madurez tecnológica de la organización, por lo que se proyecta aplicar.

El Marco referencial COBIT, adaptado a Seguros del Pichincha s.a., que se sujeta a prácticas de administración a través de objetivos de control de "Alto Nivel", organizadas en

Evaluar, dirigir y monitorear

Alinear, planear y organizar

Construir, adquirir e implementar

Entrega, servicio y soporte
Monitorear y evaluar activos

Cada uno de estos dominios contiene declaraciones de los resultados que se deseen obtener, mediante la implementación de procedimientos de controles específicos y relacionados a la actividad TI, en función de los riesgos identificados y focalizados en el departamento de recursos informáticos de Seguros del Pichincha s.a.

La técnica que se propone servirá para entender los numerosos aspectos que se relacionan con los procedimientos de una auditoria informática en seguridad de la información lo que permitirá realizar de forma adecuada. Cabe mencionar que para el adecuado desarrollo de los procedimientos se estudiaran algunas técnicas que existen en la actualidad.

1.2.4. COBIT 5

Isaca (2012) Conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI). COBIT 5 provee un Framework de Gobierno y Gestión de TI para las empresas.

COBIT es un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT.

La última versión de COBIT fue liberada en abril de 2012, esta última versión consolida e integra los marcos de trabajo COBIT 4.1, Val IT 2.0 y Risk IT, y también se basa significativamente en el marco de trabajo de aseguramiento de TI de ISACA (ITAF) y el Modelo de Negocio para la Información de Seguridad (BMIS). Sigue en línea con los marcos de trabajo y estándares como ITIL, ISO, PMBOK, PRINCE2 y FFIEC.

Beneficios de COBIT 5:

Mantiene información de alta calidad para soportar las decisiones de negocio.

Alcanzar los objetivos estratégicos y obtener los beneficios de negocio a través del uso efectivo e innovador de TI.

Lograr la excelencia operativa a través de una aplicación fiable y eficiente de la tecnología.

Mantener los riesgos relacionados con TI a un nivel aceptable.

Optimizar el costo de servicios de TI y tecnología.

Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas.

Principios de COBIT 5

El marco de COBIT 5 se basa en 5 principios clave que incluyen una amplia guía para los facilitadores de gobierno y gestión de TI en la empresa. En la Figura 1.2 se muestran estos 5 principios.

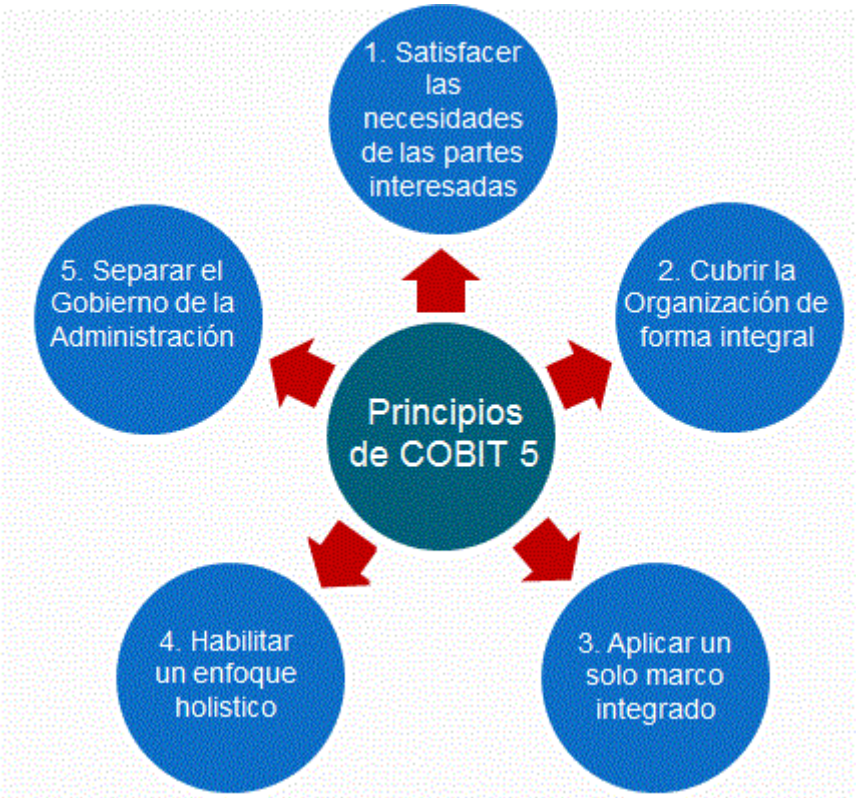


Figura 1.2. Principios de COBIT 5
Fuente: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

COBIT 5 define 7 categorías de habilitadores que se pueden ver en la Figura 1.3:

Figura 1.3. Habilitadores de COBIT 5
Fuente: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

Principios, Políticas y Marcos: Son el vehículo para trasladar el comportamiento deseado en guías prácticas para la gestión diaria.

Procesos: Describen un conjunto de prácticas y actividades organizadas para cumplir con ciertos objetivos y producir un conjunto de salidas para alcanzar los objetivos generales relacionados con TI.

Estructuras Organizacionales: Son las entidades claves en la toma de decisiones de la empresa.

Cultura, Ética y Comportamiento: La cultura, ética y comportamiento de los individuos y de la empresa muchas veces son sobrestimados como un factor de éxito en las actividades de gobierno y gestión.

Información: Requerida para mantener la empresa en ejecución y bien gobernada. En el nivel operacional, la información es un producto clave de la empresa.

Servicios, Infraestructura y Aplicaciones: Incluye la infraestructura, la tecnología y las aplicaciones para proveer a la empresa los servicios y procesamiento de Tecnología de la Información.

Personas, Habilidades y Competencias: Requeridas para completar con éxito las actividades y para tomar las decisiones correctas y acciones correctivas.

COBIT 5 hace una clara distinción entre gobierno y gestión. Estas dos disciplinas abarcan diferentes tipos de actividades, requieren de estructuras organizativas diferentes y tienen objetivos diferentes. Para este marco la diferencia clave entre gobierno y gestión es:

Gobierno: asegura que las necesidades de los Stakeholders, condiciones y opciones son evaluadas para determinar un balance entre el logro de los objetivos estratégicos de la organización; establecer dirección de la organización a través de priorización y toma de decisiones; y monitorear el desempeño y cumplimiento contra la dirección y los objetivos acordados. En la mayoría de las empresas, el gobierno es responsabilidad de la junta directiva bajo el mando del presidente.

Gestión: planea, construye, ejecuta y monitorea actividades en alineamiento con la dirección establecida por gobierno, para alcanzar los objetivos estratégicos de la organización. En la mayoría de las organizaciones, gestión es responsabilidad de la dirección ejecutiva bajo el mando del CEO.

Procesos de TI.

COBIT se divide en tres niveles:

Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.

Actividades: Acciones requeridas para lograr un resultado medible.

En detalle, el marco de trabajo general COBIT se muestra gráficamente en la Figura 2.6, con el modelo de procesos de COBIT compuesto de cinco dominios que contienen 37 procesos facilitadores, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

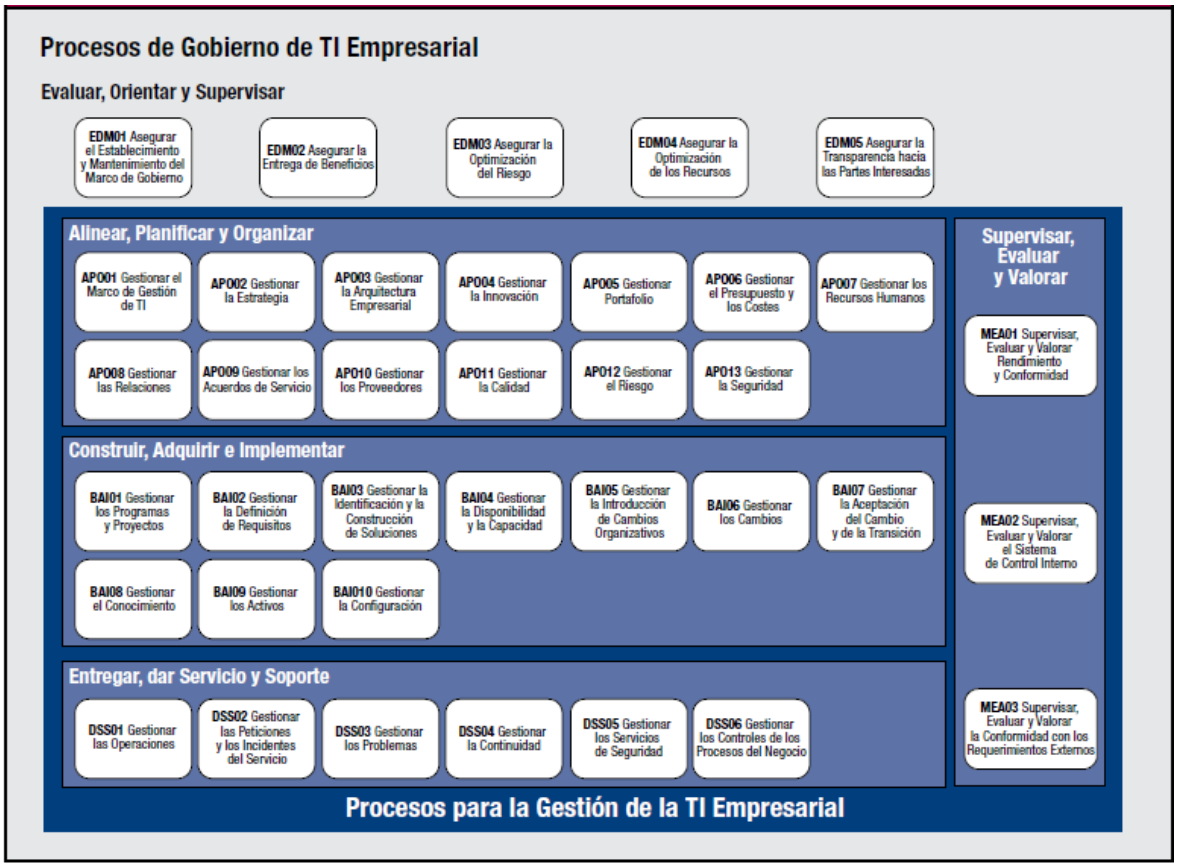


Figura 1.4. Marco de Trabajo Completo de COBIT.
Fuente: (COBIT 5,2012, p. 33)

El Marco de Trabajo COBIT 5.

COBIT 5 es un marco de trabajo integral para el gobierno y gestión de las TI corporativas. Tiene como objetivo principal, ayudar a las empresas a generar el valor óptimo desde las TI manteniendo el equilibrio entre los beneficios y la optimización de los niveles de riesgo y el uso de recursos. (ISACA, 2012)

COBIT 5 corresponde a la última versión del marco de trabajo publicado y mantenido por ISACA, una asociación global, independiente sin fines de lucro que se involucra en el desarrollo, adopción y uso, de conocimiento y prácticas mundialmente aceptadas en la industria de los SI.

La Figura 1.5 detalla los productos que conforman la familia COBIT 5, la cual incluye el propio marco de trabajo y otras publicaciones que proporcionan orientación adicional sobre los catalizadores dentro del marco o guías profesionales que se pueden utilizar de acuerdo a las necesidades de cada empresa.

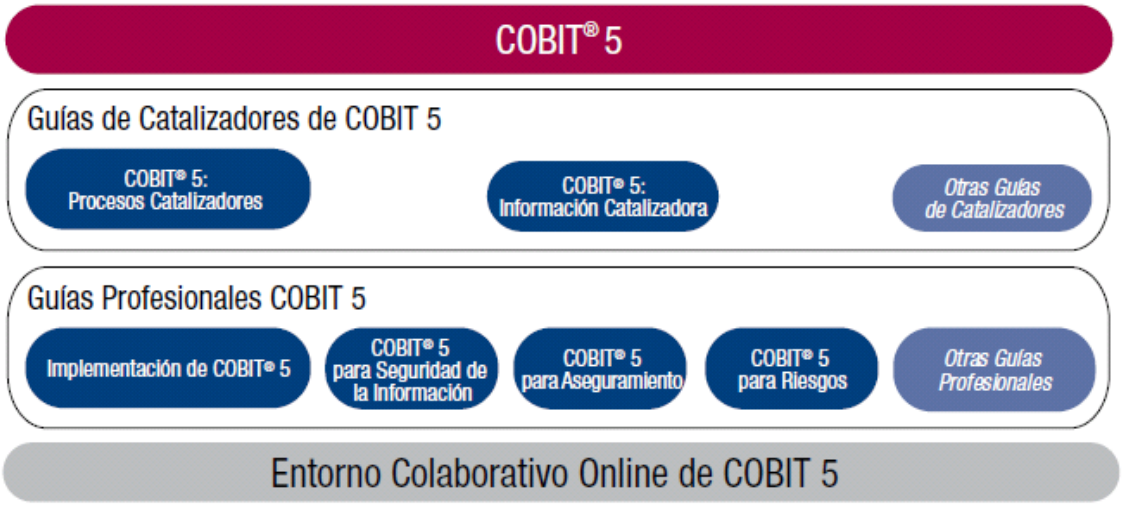


Figura 1.5. Familia de Productos COBIT.
Fuente: (COBIT 5,2012, p. 36)

Los catalizadores de COBIT 5.

Los catalizadores son cualquier elemento que puede ayudar o facilitar la consecución de las metas de la empresa, por tanto son factores que influyen en el éxito o fracaso de una actividad. Los catalizadores son guiados por la cascada de metas y se rigen a las características explicadas en ese punto.

El marco de trabajo COBIT 5, considera 7 categorías de catalizadores tal como se muestra en la Figura 1.6

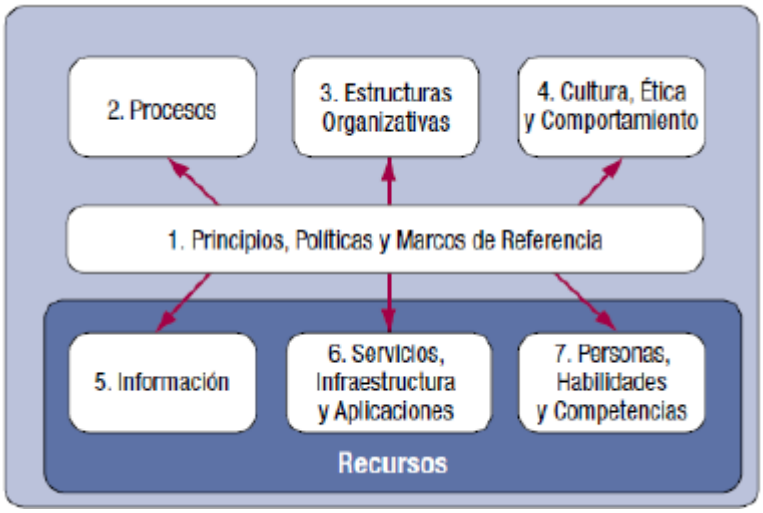


Figura 1.6. Categorías de Catalizadores COBIT.
Fuente: (COBIT 5,2012, p. 39)

1.2.5 COSO, Committee Of Sponsoring Organizations Of The Treadway Commission COSO Report o COSO I fue un informe sobre control interno elaborado en 1992 por el Committee of Sponsoring Organizations of the Treadway Commission de los EEUU., con el objetivo fundamental de especificar un marco conceptual de control interno de las organizaciones, capaz de integrar las diferentes políticas y lineamientos que permitan a la alta dirección mejorar sus sistemas de control interno. De acuerdo a COSO I, el control interno se basa en los siguientes componentes: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y supervisión.

El COSO II O COSO ERM (Enterprise Risk Management) fue formulado en el 2004, su enfoque es el mismo que el de COSO Report pero basado en el riesgo.

Este nuevo enfoque no sustituye el marco de control interno, sino que lo incorpora como parte de él, permitiendo a las organizaciones mejorar sus prácticas de control interno o decidir encaminarse hacia un proceso más completo de gestión de riesgo.

Marco del Control Interno (COSO-ERM: La definición del marco del control interno se entiende como el proceso que ejecuta la administración con el fin de evaluar operaciones específicas con seguridad razonable en tres principales categorías: Efectividad y eficiencia operacional, confiabilidad de la información financiera y cumplimiento de políticas, leyes y normas. (COSO, 2004)

La comprensión del control interno puede así ayudar a cualquier entidad pública o privada a obtener logros significativos en su desempeño con eficiencia, eficacia y economía, indicadores indispensables para el análisis, toma de decisiones y cumplimiento de metas. (COSO, 2004)

El marco integrado de control que plantea el COSO-ERM consta de ocho componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión, siendo estos componentes siguientes: ambiente interno, establecimiento de objetivos, identificación de eventos, evaluación de riesgos, respuesta al riesgo, actividades de control, información y comunicación, y supervisión.

La gestión de riesgos empresariales no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro.

Existe también una relación directa entre los objetivos y los ocho componentes referenciados, la que se manifiesta permanentemente en el campo de la gestión: las unidades operativas y cada agente de la organización conforman secuencialmente un esquema orientado a los resultados que se buscan. Un cuadro de las componentes se muestra en la Figura 1.7 (COSO, 2004)

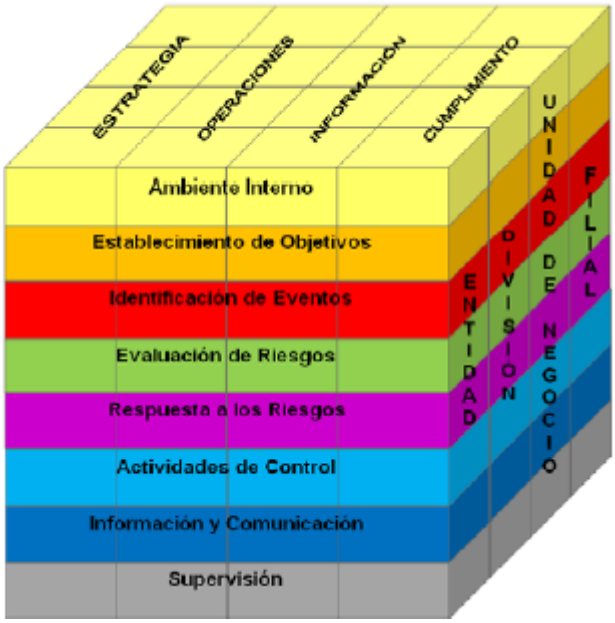


Figura 1.7. Componentes de COSO-ERM.
Fuente: (NASAudit, 2009, p.2)

Debe existir una circulación multidireccional de la información: ascendente, descendente y transversal, además de líneas abiertas de comunicación y una clara voluntad de escuchar por parte de los directivos. La Figura 1.8 Expone los flujos de información entre actividades inherentes a la gestión de riesgos empresariales de forma conceptual.

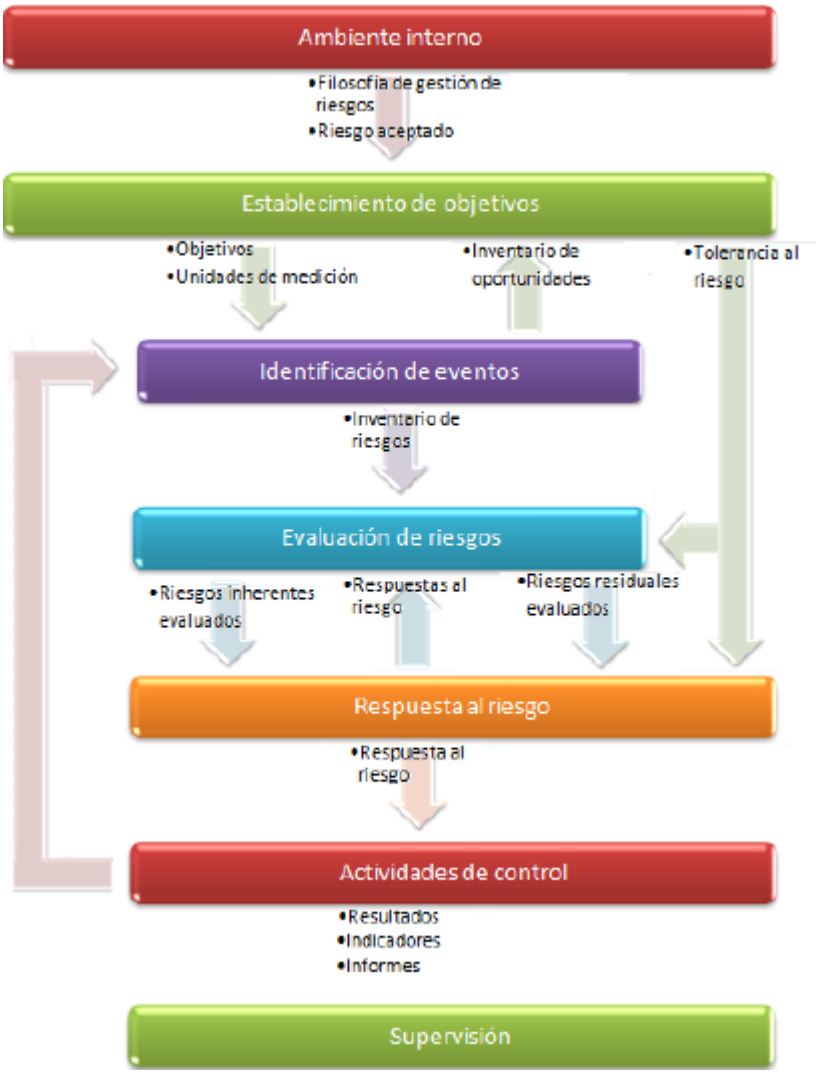


Figura 1.8. Flujos de Información ERM.
Fuente: (COSO, 2004, p.87)

1.2.6 ITIL

Information Technology Infrastructure Library (‘Biblioteca de Infraestructura de Tecnologías de Información’), frecuentemente abreviada ITIL, es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI.

Aunque se desarrolló durante los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990. SI es una certificación. ITIL se considera a menudo junto

con otros marcos de trabajo de mejores prácticas como la Information Services Procurement Library (ISPL, 'Biblioteca de adquisición de servicios de información'), la Application Services Library (ASL, 'Biblioteca de servicios de aplicativos'), el método de desarrollo de sistemas dinámicos (DSDM, Dynamic Systems Development Method), el Modelo de Capacidad y Madurez (CMM/CMMI) y a menudo se relaciona con la gobernanza de tecnologías de la información mediante COBIT (Control Objectives for Information and related Technology).

El concepto de gestión de servicios de TI, aunque relacionado con ITIL, no es idéntico: ITIL contiene una sección específicamente titulada «Gestión de Servicios de TI» (la combinación de los volúmenes de Servicio de Soporte y Prestación de Servicios, que son un ejemplo específico de un marco ITSM), pero sin embargo es importante señalar que existen otros marcos parecidos. La Gestión de Servicio ITIL está actualmente integrado en el estándar ISO 20000 (anterior BS 15000).

ITIL se construye en torno a una vista basada en proceso-modelo del control y gestión de las operaciones a menudo atribuida a W. Edwards Deming. Las recomendaciones de ITIL fueron desarrolladas en los años 1980 por la Central Computer and Telecommunications Agency (CCTA) del gobierno británico como respuesta a la creciente dependencia de las tecnologías de la información y al reconocimiento de que sin prácticas estándar, los contratos de las agencias estatales y del sector privado creaban independientemente sus propias prácticas de gestión de TI y duplicaban esfuerzos dentro de sus proyectos TIC, lo que resultaba en errores comunes y mayores costes.

ITIL fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI. Los nombres ITIL e IT Infrastructure Library ('Biblioteca de infraestructura de TI') son marcas registradas de la Office of Government Commerce ('Oficina de comercio gubernamental', OGC), que es una división del Ministerio de Hacienda del Reino Unido.

Uno de los principales beneficios propugnado por los defensores de ITIL dentro de la comunidad de TI es que proporciona un vocabulario común, consistente en un glosario de término precisamente definidos y ampliamente aceptados.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de las TI para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios TI de calidad que se correspondan con los objetivos del negocio, y que satisfaga los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI.

La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por mantenimiento y operaciones.

Brindar conocimientos fundamentales de ITIL, lograr familiaridad con los procesos y temas organizacionales claves relacionados con la Administración de Servicios de IT, mostrar el vocabulario estandarizado para describir los procesos de Administración de Servicios, lograr un entendimiento de la relevancia de la Administración de Servicios en su Organización y preparar el examen ISEB/EXIN Foundation Certificate in IT Service Management.(M@rtIn´s,2008)

Figura 1.9. Biblioteca de Infraestructura de la Información
Fuente: https://seguinfo.wordpress.com/2008/12/03/%C2%BFque-es-itil-2/

CAPÍTULO II

2. METODOLOGÍA Y DIAGNÓSTICO DE LA INVESTIGACIÓN

2.1. Fuentes de información

Para desarrollar los indicadores se necesitan datos, siendo indispensable identificar la fuente de información de donde las obtendremos. Las principales fuentes de información, en el área investigada serian:

Fuente de información de acuerdo al origen de la información

Fuente de información de acuerdo con el nivel informativo o contenido

2.2. Metodología de la investigación

El presente trabajo, describe la Auditoría Informática de los Sistemas de Tecnología e Información a realizar a Seguros del Pichincha s.a. Compañía de seguros y reaseguros. Utilizando la metodología COBIT, "una herramienta desarrollada para, ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías, las buenas prácticas de COBIT están enfocadas en el ambiente de control óptimo que debe tener una empresa para de esta manera lograr una alineación efectiva entre TI y los objetivos de negocio. El fin de esta revisión técnica es identificar debilidades y emitir recomendaciones que permitan minimizar riesgos.

Para llevar a cabo la presente Auditoría, se realizaron las siguientes actividades:" (Isaca, 2014)

- Entregar un listado de requerimientos a la entidad a ser auditada.

- Revisar la documentación entregada al Equipo de Auditoría.

- Se formularan preguntas, con el fin de aclarar ciertos puntos de la documentación.

- Se elaboraran encuestas al personal de la entidad.

- En base a los resultados obtenidos, se llevaron a cabo las entrevistas que constituye un método de auditoría personalizada, para profundizar en la indagación.

- Tomando como base las encuestas y las entrevistas, se elaboraron las pruebas sustantivas (checklist) y se recopilaron evidencias.

- De acuerdo a los resultados obtenidos en las encuestas, entrevistas y pruebas sustantivas y, alineando todos estos resultados con cada objetivo de control, que

propone COBIT, se presentaron las observaciones y recomendaciones emitidas en un informe a la Gerencia. (ISACA, 2014).

2.3. Técnicas e instrumentos de recolección de datos

En la Auditoria Informática vamos hacer referencia a las siguientes técnicas e instrumentos de recolección de datos:

Análisis y revisión bibliográficos.- Para recopilar información de libros, textos y documentos relacionados y apropiados con la problemática de la investigación.

Lectura crítica.- Para determinar los contenidos teóricos y metodológicos que permiten de forma adecuada la investigación y sus instrumentos respectivos.

Consulta de fuentes secundarias.- en caso de que sea necesario incrementar la información en las diferentes etapas y capítulos de la investigación.

Entrevistas.- De manera especial a los Funcionarios de alto rango de la institución, objeto de estudio y a quienes directa o indirectamente tienen relación con los Sistemas de Información que soporta la infraestructura tecnológica.

Cuestionarios.- Para obtener información puntual de quienes participan en los procesos que permiten dar cumplimiento a los objetivos de control y objetivos institucionales

Listas de Verificación.- Servirán para determinar el nivel de cumplimiento de Seguros del Pichincha de los objetivos de control planteados por el modelo de gestión y control COBIT 5.

2.4. Plan de Muestreo

La encuesta será aplicada a los empleados de Seguros del Pichincha de la matriz.

$$n = \frac{Z^2 * p * q}{e^2 (N-1) + o^2 * p * q}$$

Dónde:

N = Tamaño de la muestra.

P y Q = Probabilidad de éxito. P y Q = 0.25

e = error muestra 5% = 0,05

Z = Constante = 1.96

o^2 = Nivel de confianza

No se utilizará la fórmula debido a que la encuesta fue realizada a los empleados de Seguros del Pichincha de la matriz, donde n= 100 personas.

Otro punto para no aplicar la fórmula es porque se aplica a una población finita y por qué el tamaño de la muestra es una parte representativa de la población de Seguros del Pichincha.

2.5. Trabajo de campo

El proceso de la auditoría informática es similar al que se lleva a cabo a los de estados financieros, en el cual, los objetivos principales son: salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales y, la utilización racional de los recursos, con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias.

Para que una auditoría sea exitosa, debe tomar en cuenta muchos de los aspectos tratados en el punto anterior. A continuación se muestra un gráfico que muestra cómo actúan conjuntamente todos los componentes, tanto de la empresa como del auditor, para que se genere una auditoría efectiva y eficaz.

Figura 2.1. Pirámide de Procesos
Fuente: Piattini Velthuis & del Peso Navarro, 2000:20

Muchos de los componentes de la pirámide nacen de un proceso de auditoría, el cual se detalla a continuación y al cual hemos dividido en 3 etapas:

Planificación de la auditoría Informática

Ejecución de la auditoría Informática

Finalización de la auditoría Informática

2.6. Procesamiento de la información

Una vez recolectada la información necesaria se procederá al análisis de los datos obtenidos los cuales son parte medular para la propuesta. Los datos serán cuantificados y presentados gráficamente y de esta forma se logrará obtener las respectivas conclusiones.

Por lo cual se realiza las siguientes encuestas las cuales están representadas gráficamente en los Anexos 1, 2, 3.

ENCUESTA A

CUESTIONARIO DE CONTROLES Y SEGURIDADES DE LOS DEPARTAMENTOS Y SECCIONES DE SEGUROS DEL PICHINCHA

CARGO: _____

DEPARTAMENTO:_____

Instrucciones: Contestar claramente y con honestidad, cada una de las preguntas que se presentan a continuación.

1. ¿La estructura actual esta óptima para que se realicen con eficiencia las funciones encomendadas?

a. Si b. No

Comentario: .....

2. ¿La estructura actual está dada para que se realicen con eficiencia el distributivo de trabajo?

a. Si b. No

Comentario: .....

3. ¿Los niveles jerárquicos actuales son necesarios y suficientes para la actividad normal del área ?

a. Si b. No

Comentario: .....

4. ¿De acuerdo a la estructura jerárquica de la empresa se tiene una adecuada comunicación entre las diferentes áreas?

a. Si b. No

Comentario: .....

5. ¿Las áreas y subdepartamentos tienen claramente establecidas sus responsabilidades?

a. Si b. No

Comentario: .....

6. ¿Los puestos de trabajo van acordes con las necesidades del área para realizar sus funciones?

a. Si b. No

Comentario: .....

7. ¿Dividen el trabajo del área en funciones?

a. Si b. No

Comentario: .....

8. ¿Se encuentra establecidas en algún documento las funciones del área?

a. Si b. No

Comentario: .....

9. ¿El personal del área participa en la elaboración de las funciones?

a. Si b. No

Comentario: .....

10. ¿Las funciones del área van acorde al reglamento interno de la organización?

a. Si b. No

Comentario: .....

11. ¿En caso de no encontrarse el jefe, un miembro inmediato puede realizar sus funciones?

a. Si b. No

Comentario: .....

12. ¿Para cumplir con las funciones del área se requiere apoyo de otras?

a. Si b. No

Comentario: .....

13. ¿Tiene conocimiento si existe doble asignación de funciones en otras áreas?

a. Si b. No

Comentario: .....

14. ¿Los objetivos están de acuerdo a las funciones del área?

a. Si b. No

Comentario: .....

15. ¿Se deja de realizar alguna actividad por falta de personal en el área?

a. Si b. No

Comentario: .....

16. ¿Se da cumplimiento por parte del personal con las políticas, procedimientos y normas establecidas en el área?

a. Si b. No

Comentario: .....

17. ¿Existen políticas para la seguridad cuando termina la relación laboral con un empleado?

a. Si b. No

Comentario: .....

18. ¿Se adapta el personal al mejoramiento administrativo del área?

a. Si b. No

Comentario: .....

19. ¿Conoce el personal el reglamento interno de trabajo del área?

a. Si b. No

Comentario: .....

20. ¿Posee el área un plan de selección de personal?

a. Si b. No

Comentario: .....

……

……

……..

GRACIAS POR SU COLABORACIÓN

ENCUESTA B

CUESTIONARIO DE CONTROLES Y SEGURIDADES FISICAS DE SEGUROS DEL PICHINCHA

CARGO: _____

DEPARTAMENTO: _____

Instrucciones: Contestar claramente y con honestidad, cada una de las preguntas que se presentan a continuación.

1. ¿El departamento donde usted trabaja tiene seguridades contra desastres naturales?

a. Si b. No

Comentario: .....

2. ¿Existe un plan de evacuación para el departamento?

a. Si b. No

Comentario: .....

3. ¿Cuentan con horarios fijos de entrada y salida?

a. Si b. No

Comentario: .....

4. ¿Se registra el acceso al departamento de personas ajenas a el?

a. Si b. No

Comentario: .....

5. ¿Existe alarmas para detectar el fuego, agua, calor o humo en forma automática?

a. Si b. No

Comentario: .....

6. ¿Existe en el departamento extintores de fuego?

a. Si b. No

Comentario: .....

7. ¿Se ha adiestrado al personal para el manejo de extintores?

a. Si b. No

Comentario: .....

8. ¿Los extintores automáticos son activados por detectores automáticos?

a. Si b. No

Comentario: .....

9. ¿Los interruptores de energía eléctrica están debidamente protegidos, etiquetados, sin obstáculos para alcanzarlos?

a. Si b. No

Comentario: .....

10. ¿Saben que hacer los brigadistas de cada departamento en caso que ocurra una emergencia ocasionada por fuego?

a. Si b. No

Comentario: .....

11. ¿Se ha adiestrado a todo el personal en la forma en que se debe desalojar las instalaciones en caso de emergencia?

a. Si b. No

Comentario: .....

12. ¿Se han tomado medidas para minimizar la posibilidad de fuego?

a. Si b. No

Comentario: .....

13. ¿Se hace mantenimiento periódico a los computadores?

a. Si b. No

Comentario: .....

14. ¿Tiene conocimiento de la existencia de un plan de contingencia?

a. Si b. No

Comentario: .....

15. ¿Los cables de red, switch, hubs, etc. Se encuentran debidamente etiquetados?

a. Si b. No

Comentario: .....

16. ¿El personal de limpieza está preparado para manipular los dispositivos informáticos?

a. Si b. No

Comentario: .....

17. ¿Existen salidas de emergencia en caso de desastres?

a. Si b. No

Comentario: .....

18. ¿Se vigila la moral y el comportamiento del personal con el fin de mantener una buena imagen?

a. Si b. No

Comentario: .....

19. ¿Existe una persona responsable de la seguridad informática en su departamento?

a. Si b. No

Comentario: .....

20. ¿Existen alarmas para detectar otras condiciones anormales en el ambiente?

a. Si b. No

Comentario: .....

……

……

……..

GRACIAS POR SU COLABORACIÓN

ENCUESTA C

CUESTIONARIO DE SEGURIDADES LOGICAS DE SEGUROS DEL PICHINCHA

CARGO: _____

DEPARTAMENTO: _____

Instrucciones: Contestar claramente y con honestidad, cada una de las preguntas que se presentan a continuación.

1. Si tiene algún problema informático

Usted comunica al Departamento de Sistemas

Lo soluciona solo

Ambos

Ninguno

2. Cuando usted abandona su lugar de trabajo

Apaga el computador

Coloca un ingreso de contraseña para reiniciar las actividades

Ninguna de las dos alternativas

3. Cada cuanto tiempo modifica la contraseña de su computador

Cada semana

Cada mes

Nunca

4. Su computador tiene un UPS

a. Si b. No

5. Como apaga su computador

Botón inicio, y opción apagar

Presiona el botón del CPU

Otro

6. Posee una contraseña personal para el uso del sistema de la empresa

a. Si b. No

7. Para el uso del Internet usted necesita

Pedir acceso al Departamento de Sistemas

Simplemente ingresa

Otro

8. Tiene conocimiento de todos los software instalados en su computador

Poco

Mucha

Nada

9. Cree que necesita una capacitación para el uso de sistemas nuevos en la empresa

a. Si b. No

10. Para instalar nuevo software en su computador

Solicita permiso al Departamento de Sistemas

Lo instala usted y lo comunica al Departamento de Sistemas

Simplemente lo instala

No lo instala

Conclusiones:

.....

……

……

……..

GRACIAS POR SU COLABORACIÓN

2.7. Análisis e interpretación de resultados.

En las encuestas realizas en las diferentes áreas se recolecto bastante información la cual evidencia grave problemas en la Seguridad informática por lo cual deberán tomar en cuenta para mejorar sus procesos.

De aquí partirá el análisis donde se identificaran los riesgos existentes y potenciales, se evidencia conclusiones sobre la situación actual.

El estudio anterior ha reconocido puntualizar un esquema minucioso basado en la situación real, y determinar una estrategia de auditoría apropiada que acceda a determinar el estado de los procesos, en principio a tres dimensiones que incluyen desempeño, madurez y cumplimiento de objetivos de control de acuerdo a COBIT.

Cada una de las dimensiones mencionadas, se basan bajo un modelo adecuado que establece indicadores cuantitativos y/o cualitativos en base a la integración de un conjunto de matrices, que cubren cada uno de los aspectos considerados en el análisis.

2.8. Problemas y especificación de requerimientos.

Es importante analizar estos aspectos, para poder establecer cómo mejorar la calidad del análisis de requerimientos. Para esto, se debe partir de la siguiente premisa: el factor más relevante en el éxito de un proceso de ingeniería de requerimientos, es la calidad con que se desarrolla el mismo. Por esto la herramienta de software se relaciona con el modelo, de manera que actúa como un elemento de soporte, para facilitar algunas actividades definidas en el modelo, únicamente en la fase de análisis de requerimientos.

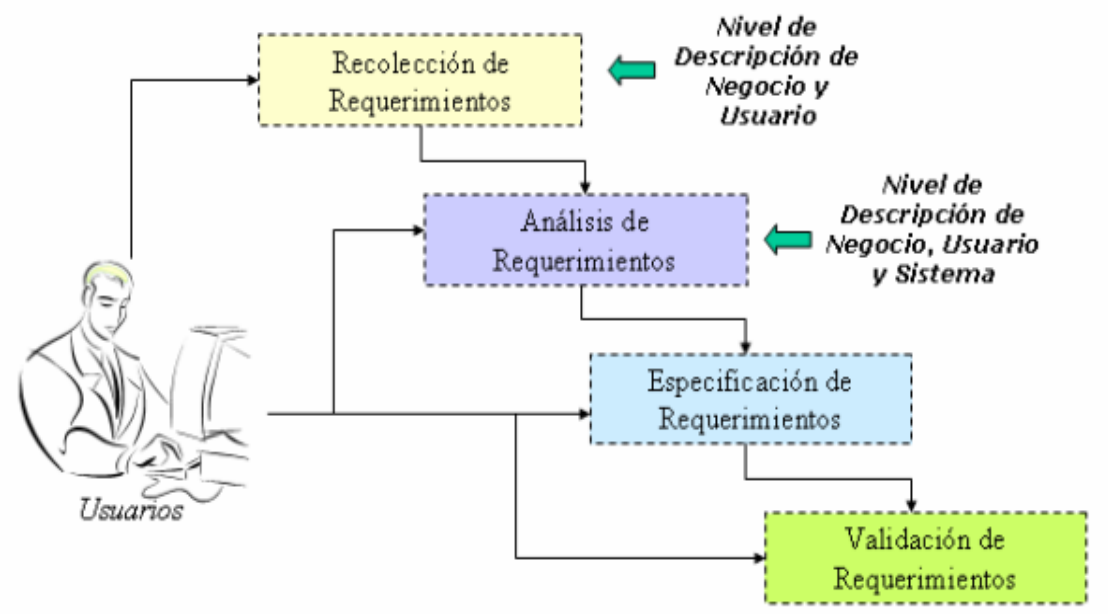


Figura 2.2. Niveles de descripción de requerimientos utilizados en las diferentes fases del proceso de ingeniería de requerimientos.
Fuente: http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis189.pdf

2.9. Estudio de Factibilidad

2.9.1. Estudio de Factibilidad Operativa

2.9.1.1 Resistencia al cambio

Para analizar la resistencia al cambio que la Auditoria Informática, motivo de esta investigación, puede generar en su etapa de investigación se ha considerado a todos los posibles usuarios que tendrán que ser consultados en el uso del software, los cuales son: Personal de administración y operaciones, Personal de Directivos y el Personal de Ventas

Se estima que la resistencia al cambio será mínima debido a que los dos primeros tipos de usuarios han solicitado La Auditoria Informática de software que les ayude a controlar la información generada.

2.9.1.2. Viabilidad de la Implementación

La implementación de la auditoria depende básicamente de tres puntos principales que son: plataformas de hardware, software y comunicaciones.

Seguros del Pichincha s.a Compañía de seguros y reaseguros posee actualmente toda la tecnología de telecomunicaciones necesaria para la correcta implementación de software sobre la cual se encuentra funcionando su red.

En cuanto al hardware la Empresa tiene a su disponibilidad varios computadores en los cuales se puede desarrollar e implementar diferentes aplicación, además de esto tiene la intención de adquirir nuevos equipos con este propósito, en caso de ser necesario.

En lo referente al software, el establecimiento está dispuesto en incurrir en gastos para la implementación del producto de software así como la compra de licencias.

2.9.1.3. Impacto Tecnológico

En el proyecto actualmente se estima que el impacto tecnológico será considerable desde ese punto de vista. Se prevé que dicho impacto será mínimo en el momento en que se realice la auditoria, ya que cualquier eventualidad sobre el mismo podrá ser gestionada directamente por el autor del proyecto de investigación.

2.9.2. Estudio de Factibilidad Tecnológica

2.9.2.1. Plataforma, Sistemas, Interconectividad.

Software

El Departamento de Sistemas de Seguros del Pichincha cuenta con los siguientes tipos de software:

Software de Sistema

Sistema Operativo Windows desde la versión Xp hasta 8 Professional y para Servidores, Windows Server 2008, además se tiene algunos equipos con sistema operativo Mac OS X.

Sistemas Operativos

TABLA DE CARACTERISTICAS DE LOS SISTEMAS OPERATIVOS				
Sistemas Operativos	Microsoft Windows xp	Windows 7	Windows 8	Mac OS
Características				
Multitarea	√	√	√	√
Seguridad		√	√	√
Soporte de diferentes protocolos	√	√	√	√
Soporte cliente y servidor	√	√	√	√
Servicios Web		√	√	√
Portabilidad	√	√	√	√
Requisitos de hardware	√	√	√	√

Tabla 2.1. Características de los Sistemas Operativos
Elaborado por el Autor

Software de Control

Tanto los servidores de Correo, Dominio, Firewall, Archivos, Impresiones que son Windows 2008 cuentan con Performance Monitor la cual es una herramienta que permite medir el desempeño de los computadores de una red.

TABLA DE CARACTERISTICAS DE LOS SISTEMAS OPERATIVOS DE LOS SERVIDORES			
Sistemas Operativos de los Servidores	Windows Server 2003	Windows Server 2008 R2	Windows Server 2012
CARACTERISTICAS			
Estabilidad		√	√
Seguridad	√	√	√
Facilidad de uso	√	√	√
Disponibilidad de Programas		√	√
Interfaz Web		√	√

Tabla 2.2. Características de los Sistemas Operativos en los Servidores
Elaborado por el Autor

Software de Aplicación

Las computadoras utilizadas en el área de sistemas como en toda la institución tienen generalmente las siguientes herramientas: Microsoft Office, Sistemas de Inventario, Sistemas de Control y Automatización para Seguros, etc.

TABLA DE CARACTERISTICAS DEL PAQUETE DE PROGRAMAS INFORMATICOS			
PAQUETES DE PROGRAMAS INFORMATICOS	Microsoft Office 2007	Microsoft Office 2010	Microsoft Office 2013
CARACTERISTICAS			
Facilidad de uso	√	√	√
Múltiple Funciones	√	√	√
Presentación en Línea		√	√
Barra de herramientas de acceso rápido	√	√	√
Vista Previa en vivo	√	√	√

Tabla 2.3. Características del Paquete de Programas Informáticos
Elaborado por el Autor

TABLA DE CARACTERISTICAS DE LOS PROGRAMAS INTERNOS	
SOFTWARE	**DESCRIPCION**
TeleSoft	Sistema informático que colabora al usuario en la visualización de la información relevante del cliente, llevando registro de las interacciones con el mismo y permitiendo generar campañas para su mantenimiento.
BSSeguros	Esta herramienta permite el ingreso de información a través de la web, para todos los productos empaquetados del modelo B2C. Así en tiempo real se puede expedir certificados de los diferentes productos, en cualquier parte del mundo. Además, permite imprimir los certificados, las facturas y el documento: "Conocer a tu cliente". Estos documentos se encuentran firmados electrónicamente.
Workplace-BPM	Sistema informático que ayuda a automatizar los procesos, implementa nuevos controles en los procedimientos, tiempos y responsables.
Gestión Seguros del Pichincha	Esta herramienta, desarrollada al interior de la organización, permite resolver temas de oportunidad en diversos aspectos como: - Cuestionarios, claves, datos personales, recepción, mensajería, control de las cotizaciones, distribución de la mensajería, catálogos, cancelaciones, autorizaciones de facturas, las pólizas de los modelos B2B, B2C y B2B2C en formato PDF, además cuenta con la factura electrónica.
BSSuministros	Es un programa de administración y control de centros de costos y materiales de entrega. Es Administrado por la Jefatura de Adquisiciones y Servicios Generales.
Activos Fijos	Es un sistema de control de activos fijos a nivel nacional, que detalla el responsables del bien. Permite un control de los materiales, equipos y mobiliario adquiridos por la empresa.
Activity Report (ABC Costos)	Este sistema tiene por objetivo registrar los tiempos dedicados a las actividades realizadas por los funcionarios de Seguros del Pichincha. Las que deben ser detalladas en horas laboradas y diariamente
Gestion&Soporte	Este sistema detalla los procesos y procedimientos del Área de Tecnología.
Correo electrónico	Sistema alterno de correo electrónico a través de redes externas.
Facturación Electrónica	Se implementó está solución para la generación de comprobantes electrónicos conjuntamente con el Servicio de Rentas internas, los documentos desarrollados en este proceso son los siguientes: • Facturas • Retenciones • Notas de crédito
Sistel: Sistema de tarificación Avaya	Este aplicativo permite el control y racionalización del gasto telefónico de la empresa. Por medio de reportes se logra un mejor control y optimización del uso telefónico, como herramienta de trabajo

Tabla 2.4. Características de los Programas Internos.
Elaborado por el Autor

Hardware

El Departamento de Sistemas de Seguros del Pichincha cuenta con el siguiente tipo de hardware:

Servidores Principal (S.O. Windows 2008, 2 procesadores XEON, 4 GB Memoria, RAID 5, Fuentes redundantes, dispositivos de cinta magnética)

Proxy Server (S.O. Windows 2008, procesador core 2 duo, 1Gb)

MAIL Server (S.O. Windows 2008, procesador core 2 duo, 1 Gb)

Servidor de desarrollo (S.O. Windows 8, 1procesador XEOM, 1 GB Memoria, dispositivos de cinta magnética)

Computadores Personales y Laptops Hp 240 en total

Impresoras Lexmark, Epson, Hp.

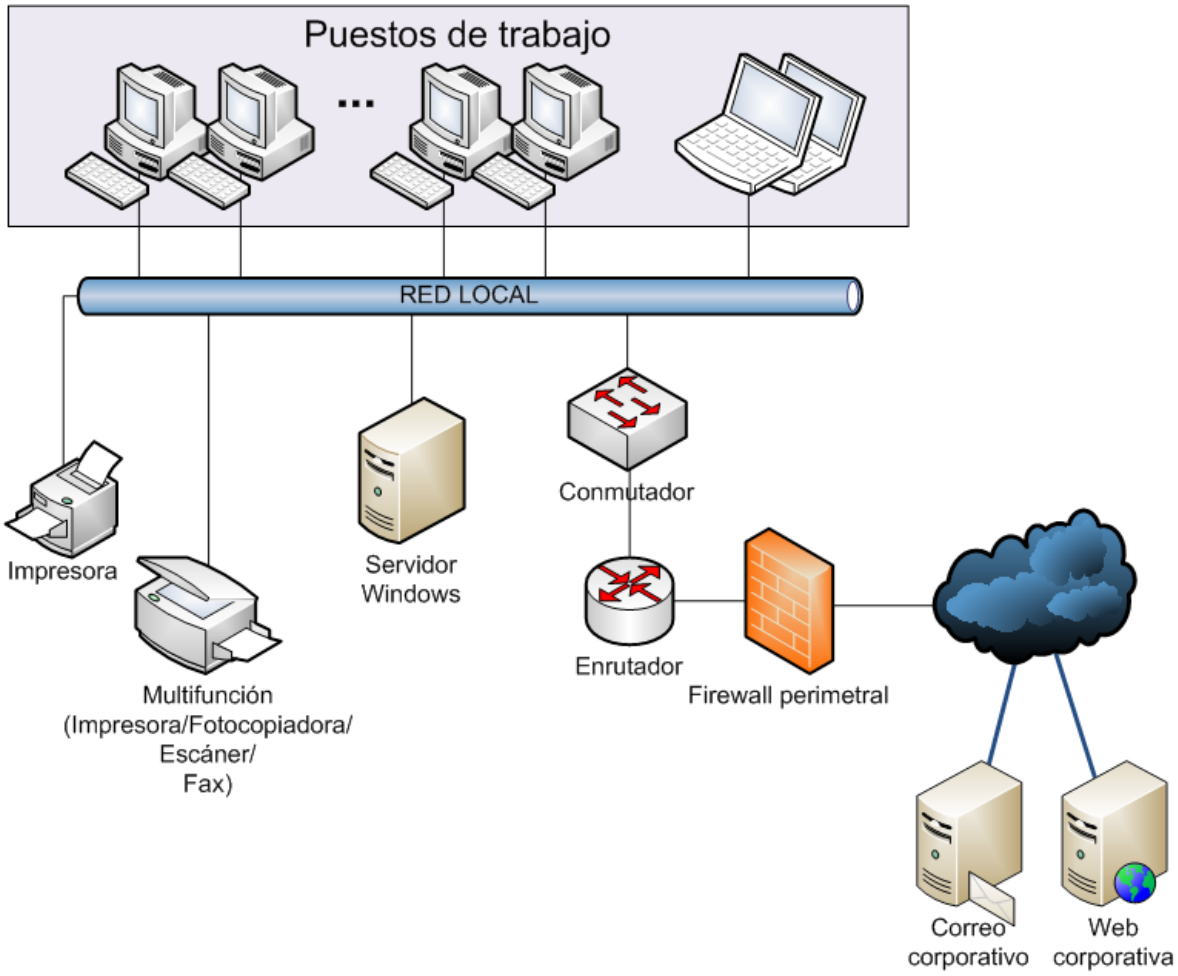


Figura 2.3. Diagrama de Servidores
Realizado por el Autor

Red

Cableado estructurado categoría 5 – 6.

Red Inalámbrica

BACKBONE de comunicaciones

Topología de Red

A continuación se describe la Topología de la red de Seguros del Pichincha s.a

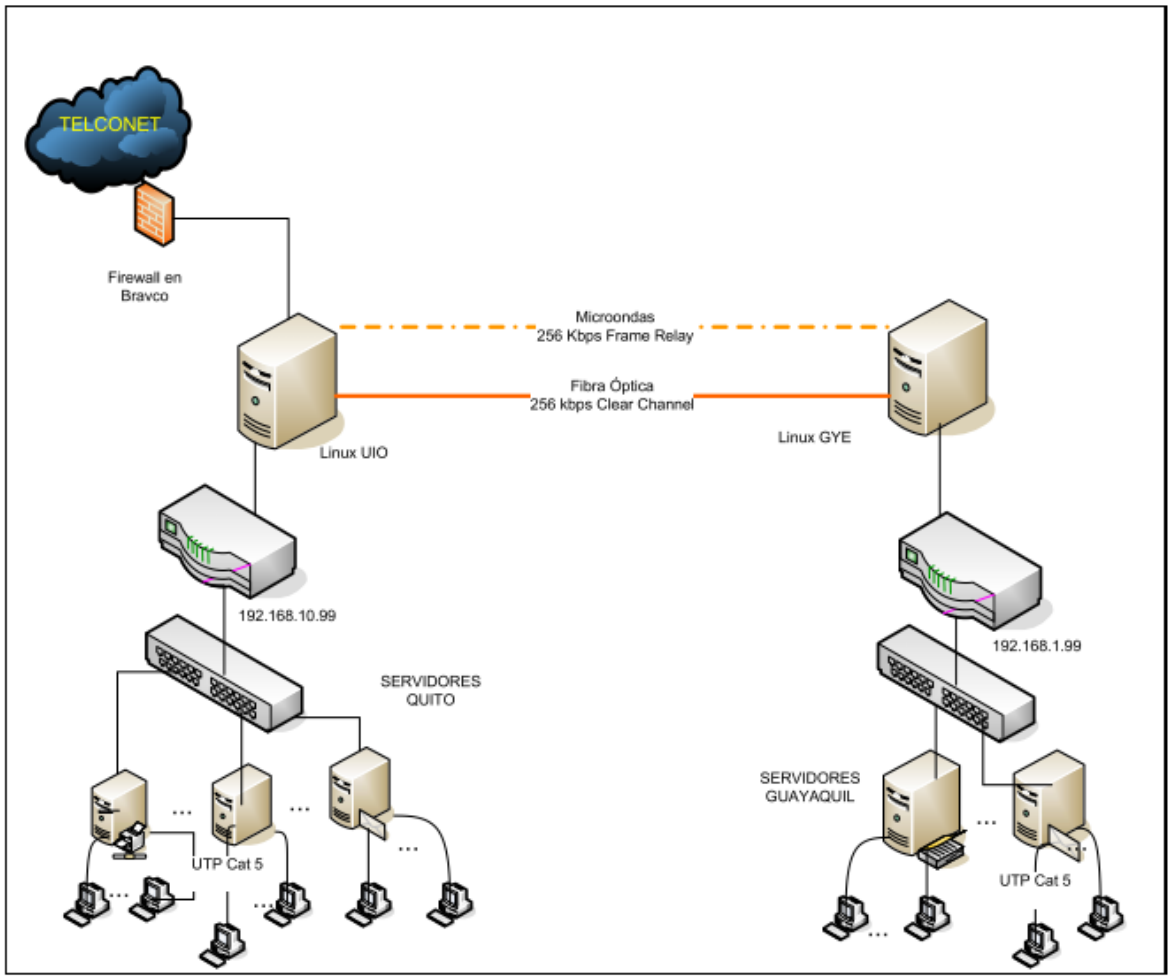


Figura 2.4. Topología de Red Seguros del Pichincha
Realizado por el autor

Topología de Red de Quito y Guayaquil, están interconectadas con dos enlaces de 256 Kbps cada uno, mediante microondas para la tecnología Frame Relay y fibra óptica para Clear Channel; Bravco es el ISP encargado de los enlaces entre Quito y Guayaquil

El Servidor de Internet se encuentra en Quito desde el cual se envía la señal a Guayaquil y demás sucursales; se tiene dos proveedores de Internet Telconet y Te Uno.

En cuanto al medio de transmisión interno utilizan UTP categoría 5 y 6, externamente fibra óptica y microondas.

2.9.3. Estudio de Factibilidad Económica

2.9.3.1. Costo de la Auditoria

Para implementar la auditoria debemos tomar en cuenta la parte económica mediante los costos del proyecto realizado en Seguros del Pichincha s.a. Compañía de Seguros y Reaseguros.

2.9.3.2. Recurso Humano

Recursos	Costo por mes $	Mes 1	Mes 2	Mes 3	Total
Jefe del Proyecto	600	600	600	600	1800
Auditor Informático	500	500	500	500	1500
TOTAL					**3300**

Tabla 2.5. Costo de desarrollo de la Auditoria Recursos humanos
Elaborado por: El Autor.

2.9.3.3 Recursos Materiales

Descripción	Cantidad	Costo Unitario	Costo Total
Impresiones	150	0.05	7.50
Anillados	3	1.20	3.60
TOTAL			**11,10**

Tabla 2.6. Costo de desarrollo de la Auditoria Recursos Materiales
Elaborado por: El Autor.

2.9.3.4. Recursos Varios

Descripción	Cantidad	Costo Unitario	Costo Total
Energía Eléctrica	1	50	50
Internet	1	30	30
Teléfono	1	15	15
Movilización	20	5	100
TOTAL			**195**

Tabla 2.7. Costo de desarrollo de la Auditoria Recursos Varios
Elaborado por: EL Autor.

2.9.3.5. Tabla Resumen

RECURSO	**COSTO INVERSION INICIAL**	**COSTO MENSUAL**	**COSTO TOTAL ANUAL**
HUMANO		1.100	3.300
MATERIALES	11,10	-	11,10
RECURSOS VARIOS	195	-	195
COSTO TOTAL	**206,10**	**1.100**	**3506,10**

Tabla 2.8. Costo total del desarrollo de la Auditoria
Elaborado por: EL Autor.

CAPÍTULO III

3. PROPUESTA

3.1. Antecedentes de la propuesta

Los Sistemas Informáticos, están integrados a la gestión empresarial por ende las normas y estándares informáticos deben estar alineados e implantados previa a la aprobación del Departamento de Sistemas de la organización, misma que se encargara de la implementación de controles de acceso a la información, que se maneja en los diversos procesos de Seguros del Pichincha s.a. en conclusión, se debe destacar que las organizaciones informáticas forman parte de la gestión de la empresa y se constituye en un elemento de apoyo en la toma de decisiones.

Actualmente la información empresarial se ha convertido en un activo fijo real invaluable, similar a la materia prima, sin embargo se debe considerar que a pesar de la capacidad que pueden tener los miembros del Departamento de Sistemas de Seguros del Pichincha s.a., la cantidad de trabajo centrado mayormente en el desarrollo de sistemas y redes, sin el personal suficiente hace que necesariamente se tomen alternativas rápidas para ganar tiempo, afectando de esta manera el servicio y por ende la calidad del producto.

Solo el 4 por ciento de los profesionales de TI han consolidado que sus empresas están preparadas para garantizar asegurar la privacidad y gobierno de Big Data[1], de acuerdo con una encuesta global hecha por la asociación profesional ISACA. Hoy la información es la divisa y las empresas no solo deben resguardarla y gestionarla, si no también usarla para generar valor para el negocio.

Para ayudar a las empresas a vencer este desafío y en el caso particular a Seguros Pichincha s.a que es nuestra entidad a utilizar el marco de negocio COBIT 5 la cual nos ofrece los siguientes beneficios principales:

Un modelo de información completo que incluye todos los aspectos de la información: usuarios, objetivos y buenas prácticas.

Una guía sobre cómo usar COBIT 5 para enfrentar los problemas frecuentes del gobierno de la información, como Big Data y las preocupaciones de privacidad.

[1] Big Data: Es un conjunto de herramientas informáticas destinadas a la manipulación, gestión y análisis de grandes volúmenes de datos de todo tipo los cuales no pueden ser gestionados por las herramientas informáticas tradicionales.

Una compresión profunda de por qué la información necesita controlarse y administrarse, junto con pasos concretos de cómo lograrlo

En Seguros del Pichincha, la información está dividida en distintos puntos aislados, se reitera en copias redundantes difundidas en la compañía y esta subutilizada por lo cual un objetivo de usar COBIT es ayudar a las compañías a simplificar el gobierno de la información para que no solo pueda manejar este trascendental activo que procede de un vasto número de canales si no también encontrar el valor de ella.

3.2. Justificación

Debido a las necesidades cada vez más cambiantes y el avance vertiginoso que a diario presenta la tecnología; se hace imprescindible que constantemente las unidades productivas y demás agentes económicos innoven sus procedimientos y técnicas para controlar sus recursos e información de manera que puedan ser más competitivos y productivos de mercado.

Por la naturaleza de Seguros del Pichincha s.a, por el volumen del flujo de fondos que administra y la rotación constante de sus transacciones se torna indispensable adoptar medidas de control de infraestructura tecnológica y herramientas de Gestión de los Sistemas que faciliten la consecución adecuada de sus operaciones y objetivos organizacionales.

Estamos frente al proceso de globalización, que si bien es cierto nos brinda la oportunidad de comercializar nuestros productos, sin embargo nos obliga a generar bienes y servicios de mayor calidad, cada vez más enmarcados en normas y estándares.

Por tal motivo, surge la necesidad de implementar en las organizaciones modelos aceptados a nivel mundial que permita controlar los recursos y aprovechar la tecnología.

Es por esto que las instituciones deben recurrir a revisiones, evaluaciones y auditorias de sistemas que se efectúen en forma periódica y que contribuyan al logro de los objetivos organizacionales, minimizando los riesgos del negocio a los que se enfrentan a diario.

Para este proyecto de investigación se utilizara el Modelo de Gestión y Control COBIT 5 para constituirse como un conjunto de las mejores prácticas de gobernabilidad de tecnologías de información, que permite a los directivos, alinear los objetivos de la infraestructura tecnológica con los objetivos propios del negocio.

Este marco de trabajo, permitirá evaluar la confidencialidad, seguridad, eficiencia, efectividad y desempeño que la institución tiene términos de tecnologías de

información, determinando los riesgos a través de niveles de madurez de los procesos con los que debería contar Seguros del Pichincha s.a para proteger sus activos mediante el cumplimiento de sus objetivos de gobierno.

Para recopilar información se realizó un estudio observacional (encuesta) en el cual buscamos recaudar datos por medio de cuestionarios previamente diseñados para obtener información primordial para un estudio preliminar de cómo se encuentra Seguros del Pichincha.

3.3. Objetivos de la propuesta

3.3.1. General

Realizar una Auditoria Informática de los sistemas de información de TI de la empresa Seguros del Pichincha s.a. Compañía de Seguros y Reaseguros, en los dominios de "Evaluar, Orientar y Supervisar, Alinear, Planificar y Organizar, Construir, Adquirir e Implementar, Entregar, dar Servicio y Soporte, Supervisar, Evaluar y Valorar", mediante el chequeo del ambiente de control, utilizando COBIT, para determinar las posibles causas y problemas que poseen.

3.3.2. Específicos

Evaluar la situación actual de la organización y su infraestructura tecnológica

Determinar el problema de los sistemas de información de TI

Determinar las causas del problema de los sistemas de información de TI

Analizar Hardware y Software de la empresa

Elaborar un informe donde se especifiquen los resultados y conclusiones de la auditoria

Proponer Soluciones al problema de los sistemas de información de TI

3.4. Desarrollo de la Propuesta.

3.4.1. Estudio Preliminar del Entorno a Auditar

La estructura organizacional de Seguros del Pichicha s.a. se sustenta en un enfoque por procesos y la filosofía de mejora continua y gestión de control de la calidad.

Misión

Desarrollar la actividad de seguros optimizando la rentabilidad de largo plazo con un servicio sobresaliente y dentro de los más altos principios de ética profesional.

Visión

Ser líderes en el mercado asegurador de personas, entregando a sus clientes servicios con valor agregado de alto impacto social, con profesionales éticos, comprometidos y en constante desarrollo; generando sólidos resultados que aporten al crecimiento económico y social del país.

"UNA FAMILIA PARA LA FAMILIA"

Valores Seguros del Pichincha

Los valores institucionales de Seguros del Pichincha son:

Respeto

Acepta, valora y actúa con mente abierta ante las diversas opiniones, creencias, culturas y formas de ser de las personas que lo rodean.

Honestidad

Capacidad para interiorizar valores éticos y morales y comportarse consecuentemente con estos.

Compromiso

Capacidad de responder con alto sentido del deber en todas las situaciones, entregando su empeño para el éxito de la empresa.

Trabajo en Equipo

Diversidad de talentos unidos con un solo propósito que colaboran y trabajan coordinadamente, empujando en la misma dirección, priorizando las metas comunes.

Liderazgo

Posee autoridad moral. Dirige, orienta, guía, tiene credibilidad, contagia entusiasmo y compromiso, obtiene eficacia del equipo; mueve la empresa. (Seguros del Pichincha, 2012)

Objetivos Estratégicos

Lograr el posicionamiento de los productos en la mente del consumidor como la compañía de protección y servicio a la familia por excelencia.
Mantener un millón de clientes satisfechos antes de finalizar la segunda década del siglo XXI.
Generar un portafolio de inversiones equivalentes al 200% de las primas recaudadas.

En resumen:

Liderar el desarrollo de SEGUROS DE VIDA.
Aprovechar y desarrollar nuevos canales de distribución de venta cruzada, así como con otras instituciones del sector financiero.
Obtener una importante participación en el mercado de seguros personales, ofertando productos estándar, de bajo costo, tanto a la familia como a la mediana y pequeña industria.
Comercializar los seguros por cuenta de terceros – vida grupo y demás, como garantía de desembolso de cualquier tipo de crédito.
Desarrollar los seguros provisionales, de salud, pensiones y otros derivados de la seguridad social, que integran mayor servicio y asistencia.

EN QUE OPERA

SEGUROS DEL PICHINCHA S.A. opera en todos los ramos o modalidades de seguros de vida y generales que se encuentran vigentes en el mercado, aprobados por la Superintendencia de Bancos. La empresa decidió trabajar con mayor énfasis en los ramos de seguros personales en los que brinda mayor servicio y, sobre todo, protección económica familiar.
A continuación se detalla los ramos que ofrece:

SEGUROS GENERALES:

Son aquellos que cubren los riesgos que causan pérdida o daños a los bienes o patrimonios y los riesgos de fianzas, garantías y fidelidad.

- Incendio y líneas aliadas.
- Robo.
- Cumplimiento.
- Responsabilidad civil.
- Todo riesgo contratista.

- Todo riesgo montaje.
- Rotura de maquinaria y lucro cesante.
- Equipo electrónico.

SEGUROS DE VIDA:

Son los que cubren los riesgos de las personas para reducir los problemas económicos derivados de la muerte del asegurado.

- Accidentes personales.
- Vida grupo
- Seguros exequial.
- Seguro educativo.
- Vida individual.

PRODUCTOS QUE COMERCIALIZA

Le empresa Seguros del Pichincha, ofrece una combinación de productos financieros y de seguros, siendo la más importante fuente de ingresos para la compañía con el producto Vida Protegida, alcanzando una penetración y desarrollo en el mercado en varios Bancos (Pichincha, Loja, Rumiñahui,) y en la entidad financiera Diners Club del Ecuador.

Seguros Vida Protegida: "VIDA PROTEGIDA" es un seguro de vida que cubre muerte por cualquier causa, no preexistente, enfermedades graves (cáncer, accidente cerebro vascular, insuficiencia renal, infarto al corazón, cirugía de arterias coronarias) anticipando hasta 50% del monto asegurado en vida, 90 días después de iniciada la videncia, y adicionalmente una asistencia en viajes que cubre al portador del seguro y a su familia en primer grado de consanguinidad en cualquier parte del mundo, protegiendo riesgos de urgencias y hospitalización en el exterior, repatriación, pérdida de equipaje y otros beneficios.

Seguros accidentes personales: Cubre la muerte accidental del asegurado con un monto a escoger de hasta USD. 60.000,00. Cubre, además incapacidad total y permanente, gastos médicos ocasionados por un accidente, indemnizaciones diarias como consecuencia de un accidente y la persona se encuentre incapacitada de trabajar.

Seguros exequiales: es el seguro que cubre los gastos ocasionados por los servicios funerarios y de entierro del asegurado y asegurados bajo esta póliza.

Seguros de vida educativa: es un seguro de vida que va dirigido hacia los estudiantes de varios Colegios de Quito que cubre muerte por accidentes personales, gastos médicos y beca estudiantil.

ESTRUCTURA ORGANIZACIONAL

La estructura organizacional de la Empresa es un pilar muy importante en la organización.

MANDOS EJECUTIVOS:

Junta General de Accionistas. Representada por los socios fundadores de la compañía, estos son Banco del Pichincha – Ecuador y Compañía de Seguros Colmena S.A. de Colombia.

Auditoría Externa. Son los encargados de verificar y controlar los registros contables y sistemas de control interno, evaluando la razonabilidad, consistencia y veracidad de las transacciones a fin de determinar desviaciones y establecer responsabilidades económico – administrativas.

Directorio. Está representado por personas nombradas por la Junta General de Accionistas como delegados de cada uno de los accionistas en la administración de la compañía.

Asesoría laboral y tributaria. Son personas externas a la compañía quienes se constituyen en un soporte para el desarrollo de las actividades relacionadas en los campos tanto laboral como tributario, por la información y conocimiento que brindan en sus asesorías.

Presidencia Ejecutiva. Tiene como misión hacer cumplir los estatutos de la Compañía, leyes, reglamentos, disposiciones y políticas fijadas por los organismos de control del Estado, la Junta General de Accionistas y el Directorio.

Gerencias. Existen ochos gerencias que tienen bajo su responsabilidad todas las funciones afines a cada área, se efectúa un proceso lógico, coherente, cronológico entre ellas y la gestión que realizan es el producto de una toma de decisiones acertada en forma continua, utilizando las mejores estrategias canalizadas hacia un objetivo común, cuyos resultados finales son presentados al Presidente Ejecutivo y éste, a su vez, presenta al Directorio y Junta General de Accionistas. Cada gerencia tiene bajo su responsabilidad a cada unidad de trabajo que es manejado por el personal calificado en cada área. Las gerencias son:

Gerencia de Planeación y Desarrollo Humano.
Gerencia Financiera.
Gerencia Técnica.
Gerencia de Marketing
Gerencia Auditoria Interna
Gerencia Austro
Gerencia Comercial.
Gerencia de Tecnología.

MANDOS OPERATIVOS:

Desarrollo Humano.

Seguros del Pichincha S.A., manteniendo criterios de calidad humana, profesionalismo y ética ha contratado personal que contribuya al desarrollo de la organización y que se identifique plenamente con sus objetivos de largo plazo.

La contratación del personal es consecuentemente con las necesidades de la compañía, así cuenta con una nómina de 200 personas de las cuales el 76% corresponden al área de mercadeo y ventas, y un 24% al área administrativa, proporción que guarda consistencia en el esquema de comercialización que mantienen.

El nivel de profesionales en la empresa ha sido una constante preocupación, ya que de ello depende en parte el dinamismo y los resultados de la empresa, es así que el 39% de los empleados tienen título universitario y el 41% se encuentran cursando una carrera universitaria o técnica.

La empresa ha sido consciente del desarrollo integral de sus empleados y que la imagen y eficiencia de la institución depende en gran medida del grado de satisfacción laboral de las personas que en ella se desenvuelven y no solo de su grado de capacitación técnica, por lo cual ha emprendido en un programa de Desarrollo Profesional y Personal, asesorado por un profesional en el campo de psicología industrial, con el propósito de alcanzar dos objetivos que son la excelencia en el trabajo y el mejoramiento de las relaciones laborales.

Otro aspecto importante es la capacitación externa al personal en temas de aplicación directa en el desempeño de funciones, propiciando así elevar el nivel de productividad. (Duque Tobar Ivonne, 2005)

GERENCIA FINANCIERA

Se desarrolla bajo los conceptos de calidad y mejoramiento continuo de procesos, procedimientos y servicios, el crecimiento de la organización fue ordenado, se cumplió con lo planificado y se dio eficiente respuesta a los requerimientos de los clientes.

Esta gerencia, realizó grandes logros para el 2013 que aportaron a los resultados de la compañía y que se reflejan en las siguientes cifras:

Con respecto a la gestión financiera, el valor del portafolio de inversiones al cierre del año alcanzó los USD $2.629.134,00, un crecimiento del 26% frente al año anterior que fue de USD $2.083.962,00. Igualmente se aprecia un crecimiento en las inversiones obligatorias de 26%, las cuales representan el 73% del total del portafolio y que ascendieron a USD $1.907.573,00, representadas principalmente en obligaciones bancarias, certificados de inversión, avales y valores fiduciarios; el 27% está constituido por inversiones voluntarias las cuales ascienden a USD $721.561,00 las mismas que crecieron en 27% con respecto al año anterior.

El producto de inversiones para el ejercicio fue de USD $117.901,00. se terminó el año 2013 encajados en inversiones obligatorias con un excedente de USD $362.563,00.

Cabe destacar que por efecto del incremento en ventas, mayor recaudo de cartera y disminución de costos financieros proyectados, en el segundo semestre de 2003 la compañía realizó un abono anticipado de USD $150.000,00 al préstamo de largo plazo que mantiene con el Banco del Pichincha.

Con respecto al control de los costos operativos y administrativos, al cierre del año tuvimos un cumplimiento del 87% con respecto al presupuesto.

GERENCIA TÉCNICA

El año 2013 fue un año positivo para la gerencia técnica en cuanto a la consolidación de los resultados que se empezaron a ver en el año inmediatamente anterior.

En la dirección de siniestros, se generó mejoramiento y documentación de los procesos a través del Sistema Integrado de seguros. Igualmente ya estamos en capacidad de obtener estadísticas de siniestralidad por diferentes perfiles para la toma oportuna de decisiones. También se logró mejorar el tiempo de respuesta a los clientes en la definición de siniestros.

El año 2013 gracias a la aplicación de todo lo anterior, se cerró con una siniestralidad del 29% comparado con el 36% del año anterior.

La dirección técnica y de mercadeo e investigación está a cargo de un director con dos ejecutivos. Esta dirección además de encargarse del análisis técnico de todos los productos actuales que soporten la generación de negocios siempre enfocados a los productos de seguros para personas.

En el año 2013 el resultado técnico de la compañía llegó a USD. $649.083 ubicándose como la segunda compañía con mejor resultado técnico dentro de las compañías de vida.

La renovación de los contratos de reaseguros nos permitió aumentar nuestra retención de primas modificando el esquema de reaseguros en los contratos de vida sin disminuir el nivel de protección de la compañía. Nuestros contratos están colocados con reaseguradores de primera línea a nivel mundial.

GERENCIA MARKETING

La Gerencia de Marketing cuenta con diferentes estudios de mercado entre otros para cumplir los objetivos de su mercadotecnia Nuestro objetivo es el diseño, estrategias de ventas de los productos de Seguros del Pichincha s.a.

GERENCIA AUDITORIA INTERNA

La Gerencia de Auditoría Interna es proporcionar servicios de aseguramiento (auditoría) y consultoría independientes y objetivos, concebidos para agregar valor y modernizar las operaciones de la compañía. Asimismo, contribuir al cumplimiento de sus propósitos, cooperando una perspectiva sistemática y disciplinada para estimar y mejorar la efectividad y eficacia de los procesos de gestión de riesgos, control y gobierno corporativo. Así mismo, realizar seguimiento y evaluación a los procesos para mejorar continuamente la eficacia y eficiencia de los sistemas de gestión de la organización con el fin de tomar acciones de mejora.

Teniendo en cuenta que todas las actividades, las operaciones y los procesos pueden someterse a un examen de auditoría interna, el alcance del trabajo de la Gerencia de Auditoria Interna será determinar si los procesos de gestión de riesgos, control y gobierno corporativo son adecuados y funcionan asegurando que:

Los riesgos están correctamente reconocidos y tratados.

Esta interacción entre los distintos grupos de dirección de acuerdo con las exigencias.

La información financiera, de gestión y operativa valiosa es concreta, confiable y exacta.

Las acciones de los funcionarios ejecutan con las políticas, normas, principios, procedimientos, leyes y regulaciones aplicables.

Los recursos se adquieren en forma económica, se utilizan eficientemente, y están adecuadamente protegidos.
Se cumplen los programas, planes y objetivos.
Las leyes o regulaciones aplicables están siendo aplicadas apropiadamente.
Durante las diferentes auditorías se identifican mejoras a la gestión del control, a los rendimientos e imagen de la Empresa. Estas mejoras se comunican al Comité de Presidencia y al Comité de Auditoría respectivamente.

Adicionalmente, la Gerencia de Auditoría Interna participará en el fortalecimiento del Sistema de Control Interno Institucional, contribuyendo a fomentar la cultura de autocontrol y autoevaluación en la organización.
Auditoria Interna se encarga a más de actividades incluidas en el programa anual de trabajo aprobado por el Directorio, a la coordinación de información de los diferentes auditores o consultores que realizan revisiones de la información de Seguros del Pichincha, como es el caso de:
Superintendencia de Bancos y Seguros
Auditores Externos
SRI
Calificadora Riesgo
Contraloría de Filiales
Auditoria del Banco Pichincha

GERENCIA AUSTRO

Esta Gerencia es la cabeza visible de la compañía en la Región Austral del país, por lo tanto replica y coordina con todas las Gerencias de Matriz

GERENCIA COMERCIAL

La Gerencia Comercial cuenta con diferentes canales de distribución así: redes financieras, mercadeo tradicional (brokers), y otros. Nuestro objetivo es siempre la búsqueda de alternativas de seguridad y protección para la familia ecuatoriana, de la mano con la rentabilidad de nuestros accionistas.

DESCRIPCIÓN DE PROCEDIMIENTOS

Un ejecutivo de Seguros del Pichincha atiende al cliente en la operación que necesite e informa del nuevo beneficio (seguro de vida), que ha creado el Banco para todos sus clientes, lo invita a pasar a su escritorio donde le explica al cliente las coberturas y amparos que tiene la póliza de Seguro de VIDA PROTEGIDA y cotiza el valor de la prima a pagar según la edad y el monto ser asegurado, tratando de persuadirlo y despertando en él la necesidad de protección con el fin de que adquiera el seguro, convencido de sus ventajas.

Una vez que el cliente accede a tomar la póliza, el ejecutivo le solicita un documento de identidad con el que verifica que el interesado cumpla con los requisitos de asegurabilidad, y que tenga el saldo necesario para el débito en la cuenta corriente o de ahorros.

El seguro entra en vigencia a partir de las 00:00 horas del día hábil siguiente en que el solicitante firme y selle la póliza, y que además le realicen el débito correspondiente.

3.4.2. Estudio del Departamento de Tecnología de la Información

Atribuciones y responsabilidades del Departamento de Tecnología de la Información

Entre las atribuciones y responsabilidades se encuentran los siguientes:

Cumplir y hacer cumplir las leyes y procedimientos en temas de gestión de tecnologías informáticas.

Contribuir en el planteamiento de servicios de tecnología de la información, en el entorno de los planes aprobados, de las normas y reglamentos vigentes.

Participar en la implementación de servicios de tecnología de la información, en el marco de los planes aprobados y de las normas y reglamentos vigentes.

Operar localmente los servicios de tecnología de la información, en el marco de las normas y reglamentos vigentes.

Intervenir en la mejora continua de los servicios, acumular localmente datos y examinar tendencias comparándolas con la línea base (acuerdos de nivel de servicio, objetivos).

Ofrecer soporte técnico de primera línea a los usuarios locales.

Ayudar la implementación de redes de datos y comunicaciones de la Empresa o Sucursales.

Administrar y controlar el uso adecuado de la tecnología de la información.

Apoyar y administrar la operación de la central telefónica.

Ejecutar los planes y dar seguimiento de los planes de tecnología de la información.

Desarrollar y administrar las aplicaciones de sistemas informáticos.

Productos Desarrollados por el Departamento de Tecnología de la Información

Los productos desarrollados por este Departamento son los siguientes

Diseñar servicios: Catálogo de servicios, SLA's (Acuerdo de Nivel de Servicio), Plan de seguridad del servicio, Documento técnico del servicio / pliegos del servicio, Acta de entrega/recepción, Plan de difusión, Servicios diseñados.

Transferir (implementar) servicios: Versión de servicio desarrollada, Versión de servicio para pruebas, Versión de servicio probada, Servicio implementado, documentado y puesto en operación. Operar Servicios: Indicadores de desempeño del servicio, Solicitud de acceso al servicio atendida, Incidente (incluye reporte de problema) resuelto, Estadísticas del servicio, Informes periódicos de gestión en el marco de los procedimientos vigentes.

Objetivos estratégicos del Departamento de Tecnología de la Información

La Tecnología de la Información es un Departamento de apoyo responsable de la administración y control de TI en el organismo, los objetivos que plantean esta dirección se muestra en la Tabla 3.1

OBJETIVOS ESTRATEGICOS TI	
Innovar tecnológicamente la institución	Desarrollar Sistemas Informáticos Dar Mantenimiento a todos los sistemas de información que lo requieran Proporcionar líneas de comunicación efectivas hacia los usuarios Dotar de herramientas tecnológicas a los usuarios, que permitan incrementar su productividad Proporcionar asesoría tecnológica para la ejecución de todos los proyectos, para que se realicen en el tiempo indicado
Anticipar las necesidades tecnológicas de la institución	Investigar tendencias que cumplan con estándares internacionales y que puedan proporcionar nuevas alternativas de servicio de valor agregado a Seguros del Pichincha s.a.
Mantener una estructura dinámica	Hacer el seguimiento del marco regulatorio para el uso, administración y control del recurso tecnológico informático de la institución Optimizar los procesos de la Dirección

Tabla 3.1. Objetivos del Departamento de TI de Seguros del Pichincha
Elaborado por TI Seguros del Pichincha

Cadena de Valor

En la Figura 3.1. Se muestra esquematizada la cadena de valor de Seguros del Pichincha.

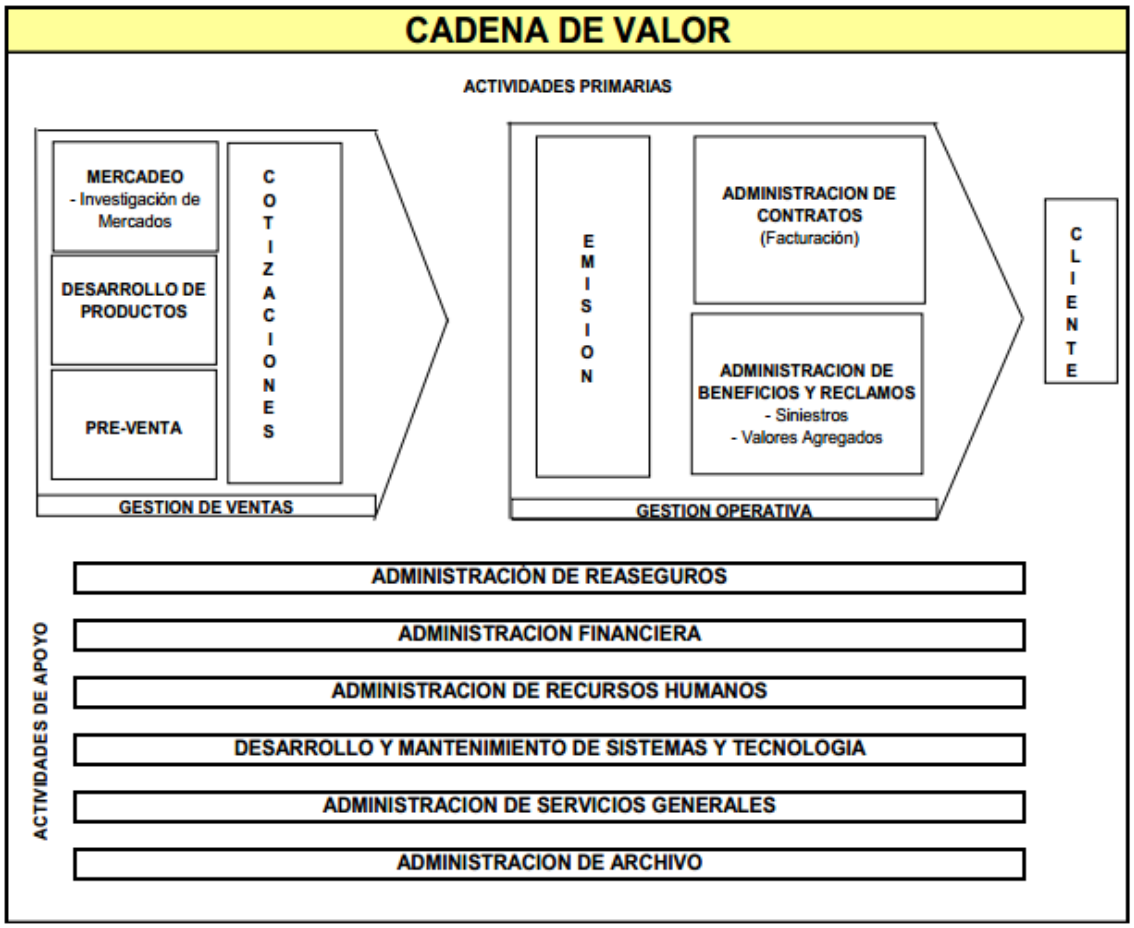


Figura 3.1. Cadena de Valor de Seguros del Pichincha
Elaborado por Seguros del Pichincha Reglamento Interno

Análisis FODA del Departamento de Tecnología de la Información

Luego de un análisis mediante observación, indagación y entrevistas se identificaron las fortalezas, oportunidades, debilidades y amenazas del Departamento de TI de Seguros del Pichincha s.a. Eso se muestra en la Tabla 3.2

FORTALEZAS	*OPORTUNIDADES*
Servidores de última tecnología, robustos y escalables, con altos niveles de fiabilidad y soporte directo de los fabricantes Diseño e implementación de un plan de tolerancia a fallos y continuidad del negocio Disponibilidad de herramientas de productividad del usuario de última generación. Redes internas de alta velocidad (Categoría 6 E) Alta inversión en renovación tecnológica	Disponibilidad en el mercado de nuevos proveedores y servicios de comunicación que ofrecen servicios de mejor calidad a menores costos Disponibilidad actual o de adquisición de herramientas que permiten reducir y controlar fugas de información interna y externa Adquisiciones de software de manejo y control de requerimientos que cumpla con políticas, estándares de documentación y SLAs. Adquisición de herramientas automatizadas de auditoria informática
DEBILIDADES	**AMENAZAS**
Percepción deficiente de ciertos usuarios de las aplicaciones Falta de administración de red que deriva en problemas estructurales , de configuración y seguridad de la red Accesos remotos débilmente controlados Deficiente aplicación de las políticas y estándares para manejo de contraseñas por los usuarios Desconocimiento de los usuarios sobre el uso de las aplicaciones y del giro del negocio Falta de un plan de capacitación permanente orientado al mejoramiento continuo del personal área Dependencia parcial de terceros sobre las aplicaciones CORE del negocio Falta de metodologías y herramientas adecuadas para manejo y documentación de requerimientos Falta de políticas de manejo de la criticidad de requerimientos y SLAs Falta de Monitoreo continuo y control de vulnerabilidades a las instalaciones de la empresa como red, centro de cómputo.	Ataques externos a las instalaciones de la empresa Ataques de virus y nuevas variantes de spam al correo de la empresa Altos costos de renovación tecnológica Mal servicio de proveedores de comunicaciones Errores y altos costos de servicios de proveedores externos Incumplimiento de proveedores

Tabla 3.2. Matriz Foda del Departamento de TI. SDP
Elaborado por TI de Seguros del Pichincha

Recursos Humanos de la Departamento general de Tecnología

Para realizar las funciones de Departamento de Tecnología que se puntualizan en el reglamento orgánico funcional por procesos descritos anteriormente, este Departamento cuenta con el recurso humano especificado en la Tabla 3.3

PUESTO DE TRABAJO DTI		
PERFIL	**CARGO ADMINISTRATIVO**	**#**
Gerencia de Tecnología	Gerente	1
Jefe de Soporte Técnico	Jefe de Tecnología	1
Jefe de Desarrollo	Jefe de Desarrollo	1
Ingeniero de Infraestructura	Ejecutivo de Soporte Tecnológico	3
Ingeniero de Desarrollo	Ejecutivo de Desarrollo	10
Asistente Técnico	Secretaria	1

Tabla 3.3. Recursos Humanos de TI
Elaborado por TI de Seguros del Pichincha

Adicionalmente, para el cumplimiento de la descentralización de funciones que se contemplan en Seguros del Pichincha s.a., se han nombrado funcionarios en las unidades regionales como muestra la Tabla 3.4

PUESTO DE TRABAJO DTI		
PERFIL	**CARGO ADMINISTRATIVO**	**#**
Soporte Regional Sur	Ejecutivo de Soporte Tecnológico	1
Soporte Regional Costa	Ejecutivo de Soporte Tecnológico	1

Tabla 3.4. Recursos Humanos de DTI-Regionales
Elaborado por TI de Seguros del Pichincha

Estructura por Procesos del Departamento de TI

La Dirección de TI, organiza su gestión por procesos, los mismos que se ajustan a ITIL V3. Una descripción detallada de ITIL se encuentra en el Capítulo 1.

Estándares establecidos en el Departamento de TI

La definición de estándares para el software, hardware, servicios de red y proveedores, busca asegurar en Seguros del Pichincha s.a. la correcta compra de los nuevos recursos tecnológicos en el área informática. La definición de marcas solo se aplica para adquisiciones definidas que no deben alterar el inventario del parque informático existente, en concordancia con lo establecido en sus procedimientos de adquisiciones, compras, etc. Para adquisiciones mayores no se aplican marcas y se deja abierta la posibilidad de adoptar nuevos lineamientos conforme a Leyes y Reglamentos.

Estándares de Software.

El software que la Gerencia General de Tecnología de la Información pone a distribución a Seguros del Pichincha, proporciona que los empleados optimicen su trabajo y cumple con las características mostradas en la Figura A1.1, del Anexo 1.

Estándares de Hardware

Los computadores de Seguros del Pichincha s.a. deben estar en condiciones mínimas de ser conectados a la red LAN principal de datos de cada administración zonal. Los dispositivos telefónicos deben ser compatibles con la central telefónica IP de CISCO. Los dispositivos y equipos que la institución compre deben cumplir requisitos mínimos de especificación de hardware. Las Figuras A1.2, a A1.6, del Anexo 1, presentan una muestra de especificaciones mínimas de hardware institucional.

Servicios Tecnológicos

La metodología de desarrollo de sistemas que emplea Seguros del Pichincha s.a. es el PROCESO UNIFICADO DE DESARROLLO DE SOFTWARE más conocido como RUP de Ivar Jacobson, Grady Booch y James Rumbaugh, por ser reconocida y aceptada mundialmente como estándar internacional.

Desarrollo

Los nuevos servicios tecnológicos de Seguros del Pichincha que se requiera, son desarrollados por el Departamento de Tecnología de la Información o por terceros bajo su coordinación y supervisión directa. Los servicios a desarrollarse, la priorización y todos sus detalles se encuentra especificados en el portafolio de servicios que forma parte del proceso de Diseño de Servicios.

Mantenimiento

Los servicios tecnológicos que posee Seguros del Pichincha necesitan mantenimiento preventivo así como la implementación de mejoras y/o control de correcto funcionamiento. Este mantenimiento lo proporciona el Departamento de Tecnología de la Información o el desarrollador del servicio con supervisión directa de éste Departamento. Se da mantenimiento de los servicios tecnológicos desarrollados por el Departamento y se proporciona asistencia, en los límites de lo posible, a todos aquellos servicios que son de desarrollo externo y que no poseen soporte contratado con el desarrollador original. En lo referente al software comercial, se solicita asistencia a los vendedores del producto o directamente a los fabricantes, de ser posible y si el caso lo requiere.

Plan de Inversión

En el plan de inversiones se proyecta la compra de software y hardware tanto de propósito general como de componentes específicos de servicios. De igual forma se contemplan las contrataciones de desarrollo de nuevos servicios y el mantenimiento de los existentes. La adquisición de software y hardware de propósito general se lo realiza de ser posible, una vez por año. La contratación de desarrollo de servicios se lo realiza según el cronograma que se defina en el portafolio de servicios atendiendo la prioridad de cada servicio. Ver Tabla 3.5.

PRESUPUESTO REFERENCIAL	
ITEM	**VALOR ANUAL**
Recurso Humano	436.890,00
Remuneración	419.250,00
Viáticos	17.640,00
Plan de Inversiones 2011	2.659.420,00
Plan de Inversiones 2012	3.765.950,00
Plan de Inversiones 2013	4.945.650,00

Tabla 3.5. Presupuesto Referencial
(Seguros del Pichincha – Plan de Inversiones, 2013)

Los valores de inversión en hardware y software no incluyen aquellos ítems definidos en los proyectos que tienen financiamiento propio así como tampoco los impuestos de ley. El rubro de viáticos corresponde a movilizaciones nacionales necesarias para la ejecución de las actividades de desarrollo y mantenimiento de servicios tecnológicos. No están considerados en este presupuesto, los montos para capacitación nacional o internacional, así como tampoco se han considerado los valores para viáticos internacionales necesarios.

3.4.3. Planeación de la auditoria informática a Seguros del Pichincha

El plan de auditoría debe estar justificado en la organización de las actividades de las entidades, sus sistemas de administración y control, la naturaleza de las transacciones, procesos que realiza y las leyes y reglamentos que aplican. El plan debe ser documentado como parte integral de los papeles de trabajo y modificado, cuando sea necesario durante el transcurso de la auditoria. El proceso de planeación comprenderá las siguientes etapas:

1. Planeación previa
2. Estudio preliminar del área a auditar.
3. Desarrollo de la estrategia de la auditoria
4. Recursos
5. Programas de auditoría

3.4.3.1. Planeación Previa

Para hacer una adecuada planeación de la auditoría en informática, se han realizado una serie de pasos previos, que permitirán dimensionar el tamaño y características del área informática dentro del organismo a auditar, sus sistemas, organización y equipo; con ello podremos determinar la estrategia, las herramientas necesarias y el tiempo, así como definir los planes y programas de trabajo para la ejecución de la auditoria. La planeación se realizará desde el punto de vista de los cuatro objetivos identificados en el

alcance: sistemas de información en operación; metodología de desarrollo o adquisición de sistemas de información; administración de hardware; y administración de telecomunicaciones. En cada una de las áreas se evaluará el desempeño y los riesgos en base al cumplimiento de los principios de seguridad, confiabilidad y eficiencia; cumplimiento de políticas y procedimientos; y en base al grado de satisfacción de la alta dirección y del personal usuario.

3.4.3.2. Estudio preliminar

El estudio inicial del entorno a auditar, realizado en los puntos anteriores, pertenece a la primera fase dentro del proceso de auditoría de acuerdo a la metodología establecida en el Desarrollo de este proyecto, ha permitido tener una percepción global y las estructuras fundamentales de la Seguros del Pichincha, así como también una perspectiva general y completa del Departamento de Tecnología de la Información.

3.4.3.3. Desarrollo de la estrategia de la auditoria

3.4.3.3.1. Determinación del Plan Estratégico de la Auditoria a Seguros del Pichincha

El plan estratégico de una auditoria informática representa la base sobre el cual estarán soportadas todas las actividades necesarias para la realización del trabajo, de modo que pueda ser alcanzado de forma eficiente. Para la realización de esta auditoría se tomará como estrategia el marco de referencia COBIT 5, analizado en el Capítulo 1.

3.4.3.3.2. Justificación del Uso del Modelo de Referencia COBIT 5

Para la ejecución de la auditoría se ha tomado como marco de referencia COBIT 5, el cual es un marco de gobernabilidad de TI y un conjunto de herramientas de colaboración que permite asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgos empresariales. Este conjunto de las mejores prácticas permiten diagnosticar la seguridad, eficacia, calidad y eficiencia de las TI., mediante lo cual se determinan los riesgos, se obtiene una gestión efectiva de los recursos, se mide el desempeño y cumplimiento de metas, y de manera principal el nivel de madurez de los procesos de la organización. Se ha elegido COBIT debido a que satisface y cumple las necesidades que tiene la organización en lo referente a las Tecnología de la Información, tomando en cuenta los requerimientos de la institución, organizando las actividades mediante el modelo de procesos, identificando los recursos de TI prioritarios a ser utilizados y definiendo los controles de TI.

3.4.3.3.3. Determinación del Marco de Trabajo de la Auditoría a Seguros del Pichincha s.a. bajo COBIT

El marco de trabajo de la auditoría a Seguros del Pichincha se enfoca y orienta hacia cuatro elementos determinantes:

1. La institución
2. Los procesos
3. Los controles
4. Las métricas, mediciones e indicadores

Orientado a la Institución: Como se vio en el Capítulo I, el marco de trabajo COBIT plantea que la institución debe invertir en controlar y administrar los recursos de TI, usando un conjunto de procesos que garanticen la alineación con los requerimientos institucionales.

Orientado a Procesos: El marco de trabajo de la auditoría informática a Seguros del Pichincha estará basado en 37 procesos definidos por COBIT, que garantizan la alineación con los requerimientos de la institución y de TI. Estos procesos se encuentran organizados en cinco dominios que se equiparan a las áreas tradicionales de Tecnologia de la Información de planear, construir, ejecutar y monitorear. Como se vio en el capítulo II estos dominios son: Evaluar, Orientar y Supervisar, Alinear, Planificar y Organizar, Construir, Adquirir e Implementar, Entregar, dar Servicio y Soporte, Supervisar, Evaluar y Valorar. (Ver figura 1.4.)

Basado en controles: La auditoría empleara 37 objetivos de gobierno generales, una para cada proceso de TI, que son políticas, procedimientos, prácticas en controles: La auditoría empleará 32 objetivos de gobierno o de gestión, uno para cada y estructuras organizacionales que proporcionan un conjunto completo de requerimientos de alto nivel para un control efectivo de cada proceso de TI.

3.4.3.3.4. Estrategia de la Auditoría Informática a Seguros del Pichincha

De acuerdo al marco de trabajo planteado en el punto anterior, la auditoría estará orientada a la institución y a los procesos de TI, empleando para su análisis objetivos de gobierno, metas. Las Tablas 3.6, 3.7 y 3.8 indican los procesos y objetivos de gobierno; las metas de TI de Seguros del Pichincha; las metas de TI de acuerdo a COBIT y las métricas y mediciones a ser empleadas en la auditoría informática a Seguros del Pichincha respectivamente. Además se brindará una visión global de cómo se relacionan las metas genéricas de la institución, con las metas de TI de acuerdo a COBIT, considerando también, los procesos de TI y los criterios de información Para establecer

esta relación entre procesos COBIT y Seguros del Pichincha, se emplearán una serie de planos que se listan en la Tabla 3.9, y se describen más adelante.

PROCESOS DE GOBIERNO DE TI	
EVALUAR, ORIENTAR Y SUPERVISAR	
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno
EDM02	Asegurar la entrega de beneficios
EDM03	Asegurar la optimización del riesgo
EDM04	Asegurar la optimización de los recursos
EDM05	Asegurar la transparencia hacia las partes interesadas
ALINEAR, PLANIFICAR Y ORGANIZAR	
APO01	Gestionar el marco de gestión de TI
APO02	Gestionar la estrategia
APO03	Gestionar la arquitectura empresarial
APO04	Gestionar la innovación
APO05	Gestionar portafolio
APO06	Gestionar el presupuesto y los costes
APO07	Gestionar los recursos humanos
APO08	Gestionar las relaciones
APO09	Gestionar los acuerdos de servicio
APO10	Gestionar los proveedores
APO11	Gestionar la calidad
APO12	Gestionar el riesgo
APO13	Gestionar la seguridad
CONSTRUIR, ADQUIRIR E IMPLEMENTAR	
BAI01	Gestionar los programas y proyectos
BAI02	Gestionar la definición de requisitos
BAI03	Gestionar la identificación y la construcción de soluciones
BAI04	Gestionar la disponibilidad y la capacidad
BAI05	Gestionar la introducción de cambios organizativos
BAI06	Gestionar los cambios
BAI07	Gestionar la aceptación del cambio y de la transición
BAI08	Gestionar el conocimiento
BAI09	Gestionar los activos
BAI10	Gestionar la configuración
ENTREGAR, DAR SERVICIO Y SOPORTE	
DSS01	Gestionar las operaciones
DSS02	Gestionar las peticiones y los incidentes del servicio
DSS03	Gestionar los problemas
DSS04	Gestionar la continuidad
DSS05	Gestionar los servicios de seguridad
DSS06	Gestionar los controles de los procesos del negocio
SUPERVISAR, EVALUAR Y VALORAR	
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad
MEA02	Supervisar, evaluar y valorar el sistema de control interno
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Tabla 3.6. Procesos y Objetivos de Gobierno COBIT.
Fuente: (COBIT 5,2012)

Metas Generales de TI-Seguros del Pichincha		
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI
	2	Gestionar los riesgos de TI que afectan a la institución
	3	Fomentar la Transparencia
Perspectiva del Cliente	4	Mejorar la orientación y servicio al usuario
	5	Ofrecer productos y servicios competitivos
	6	Establecer continuidad y disponibilidad de servicios
	7	Crear agilidad en la respuesta a los cambios de los requerimientos institucionales
	8	Lograr optimización de costos en la entrega de servicios
	9	Obtener información fiable y útil para tomar decisiones estratégicas
Perspectiva Interna	10	Mejorar y mantener funcionalidad de los procesos institucionales
	11	Reducir el costo de los procesos
	12	Proporcionar cumplimiento con leyes, reglamentos y regulaciones
	13	Proporcionar cumplimiento con políticas internas
	14	Gestionar cambios institucionales
	15	Mejorar y mantener operatividad en el control de las telecomunicaciones
Perspectiva de Aprendizaje y Crecimiento	16	Gestionar productos e innovación en la institución
	17	Adquirir y mantener personal cualificado y motivado

Tabla 3.7. Metas Generales de TI de Seguros del Pichincha
Elaborado por TI de Seguros del Pichincha

Metas de Información y Tecnología Relacionada		
Financiera	1	Alineamiento de TI y estrategia de negocio
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionas con TI
	4	Riesgo del negocio relacionados con la TI gestionados
	5	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI
	6	Transparencia de los costes, beneficios y riesgos de la TI
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	9	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Tabla 3.8. Metas de TI – COBIT
(COBIT 5, 2012)

Métricas y Mediciones de la Auditoria Informática a Seguros del Pichincha		
CALIFICADORES	**MODELOS**	**MATRICES**
Calificador Real del Estado del Proceso	MODELO MADUREZ	Matriz de Grados de Madurez de Procesos- Seguros del Pichincha
	MODELO DE MEDICION DEL DESEMPEÑO	Matriz de Nivel de Servicio – Seguros del Pichincha.
	MODELO DE MEDICION DE LOS OBJETIVOS DE GOBIERNO	Matriz de Cumplimiento de Objetivos de Gobierno - COBIT
Impacto del Proceso	MODELOS DE IMPACTO	Matriz de Impactos de Procesos frente a los criterios de información de COBIT. Matriz de Diagnostico de Procesos COBIT

Tabla 3.9. Métricas y Mediciones de la Auditoria Informática a Seguros del Pichincha (COBIT 5, 2012)

Mapa de Relación COBIT-SEGUROS DEL PICHINCHA	
Planos de Mapeo	**Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información**
	Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información
	Plano de Enlace de las Metas relacionados con las TI y los procesos relacionados con TI
	Plano de Enlace de las metas corporativas de COBIT 5 y las metas relacionadas con las TI
	Plano de Responsabilidades de Procesos COBIT

Tabla 3.10. Componentes del Mapa de Relación COBIT-Seguros del Pichincha Elaborado por el Autor

Calificador Real del Estado del Proceso

La auditoría determinara un calificador real del estado de cada uno de los 37 procesos de acuerdo a tres dimensiones: madurez, desempeño y cumplimiento de objetivos.

A su vez, cada dimensión tendrá un indicador cuantitativo, que se alcanzará de acuerdo a los modelos planteados en la sección siguiente. Como se trata de un espacio tridimensional, el calificador real del estado del proceso se obtendrá mediante la magnitud del vector resultante equivalente para indicadores con valores del 100% en las tres dimensiones. Las componentes vectoriales en i,j y k corresponden a los indicadores resultantes de las dimensiones: madurez (i), desempeño (j), y cumplimiento de objetivos (k), respectivamente. Esto se muestra en la Figura 3.2

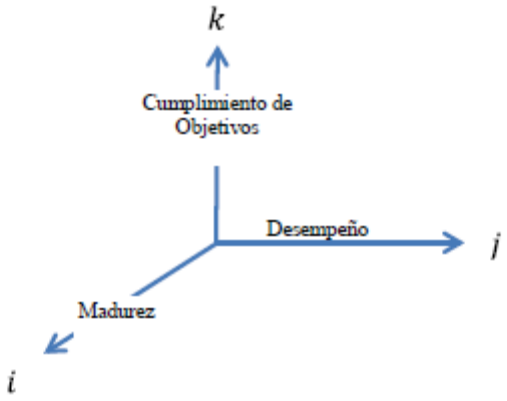


Figura 3.2. Dimensiones del Estado del Proceso
Elaborado por el Autor

La magnitud del vector resultante con valor de 100% en los indicadores de cada dimensión seria:

$$C_{ideal} = \sqrt{i^2+j^2+k^2}$$

$$C_{ideal} = \sqrt{100^2+100^2+100^2}$$

$$C_{ideal} = \sqrt{3}\ 100 = 173.21$$

Se obtiene C_{ideal} igual a $\sqrt{3}(100)$ por lo tanto para mantener 100% como valor referencial se deberá dividir por $\sqrt{3}$ el valor obtenido

Es así que la magnitud del calificador real del estado del proceso se obtendrá mediante la siguiente expresión:

$$C = \frac{\sqrt{m^2+d^2+o^2}}{\sqrt{3}}$$ Calificador Real

Donde m=% Madurez (Grado de Madurez), d=% Desempeño y o=% Cumplimiento de Objetivos

El análisis vectorial tridimensional, además de un indicador global obtenido mediante el modulo del vector (C), nos brindara información adicional respecto al sentido y dirección del mismo.

Los valores de los indicadores de Madurez, Desempeño y Cumplimiento de Objetivos son siempre positivos por lo cual el sentido corresponderá siempre a un valor resultante positivo

La dirección del vector se encaminara dada por los ángulos alfa, beta y gama con respecto a los ejes cartesianos como sigue:

$$\alpha = \cos^{-1}\ m_{C}$$

$$\beta = \cos^{-1}(d_{C})$$

$$\gamma = \cos^{-1}(o_{C})$$

Si consideramos el caso ideal

$$\alpha = \cos^{-1}\ \frac{100}{100\ \overline{3}}$$

$$\alpha = \cos^{-1}(1_{\sqrt{3}}) = 54{,}74°$$

$$\beta = \cos^{-1}\ \frac{100}{100\ \overline{3}}$$

$$\beta = \cos^{-1}(1_{\sqrt{3}}) = 54{,}74°$$

$$\gamma = \cos^{-1}\ \frac{100}{100\ \overline{3}}$$

$$\gamma = \cos^{-1}(1_{\sqrt{3}}) = 54{,}74°$$

La información alcanzada del análisis de los ángulos es también destacada ya que el ángulo con mayor valor corresponderá a la dimensión más débil del proceso.

Impacto Real del Proceso

Este indicador corresponde a un valor porcentual que determina el impacto real del proceso dentro del Departamento de TI de Seguros del Pichincha, determinado por el indicador obtenido mediante el modelo de impactos. Se dará un valor cualitativo al valor porcentual del indicador de impacto en base a las equivalencias mostradas en la Tabla 3.11.

IMPACTO	
Alto	68 -100
Medio	34 – 67
Bajo	0 – 33

Tabla 3.11.Equivalencias del Impacto (COBIT 5, 2012)

3.4.3.3.5 Descripción de los Modelos de Medición

MODELO DE MADUREZ

La aplicación del modelo de madurez permitirá identificar:

El desempeño real de la institución

El objetivo de mejora de la institución

El incremento en la madurez reduce el riesgo y mejora la eficiencia, generando menores errores, más procesos predecibles y en uso rentable de los recursos,

Indicador de Madurez (m)

Para obtener el indicador de madurez de un proceso COBIT, se empleara la matriz especificada en la tabla 3.12

INDICADOR DE MADUREZ		
PARAMETRO		**MATRIZ**
1	Grado de madurez real para un nivel i (m_{ri})	Matriz de grados de Madurez de Procesos Seguros del Pichincha.

Tabla 3.12. Parámetros del indicador de Madurez
(COBIT 5, 2012)

El indicador de madurez, el que se empleara para el cálculo del calificador global y se obtiene de la siguiente manera:

$$m = \ \ i - 1 \ \ * 20\% + (20\% * m_{ri}$$

Donde $m = Grado\ de\ Madurez, m_{ri}$ =Grado de Madurez Real correspondiente a un Nivel i.

Se utiliza la constante 20%, dado que son 5 niveles, excluyendo el no existente (0). Por tanto $\frac{100\%}{5} = 20\%$. Esto es para el Nivel 0 = 0%, Nivel 1 = 20%, Nivel 2= 40%, Nivel 3 = 60%, Nivel 4 = 80%, Nivel 5 = 100%.

Para determinar las medidas que definan un nivel de madurez especifico, se utilizara las recomendaciones descritas en el marco de trabajo de COBIT.

Modelo de medición del desempeño

La medición del desempeño es fundamental para el gobierno de TI. COBIT le da soporte e incluye la institución y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso).

Indicador de Desempeño (d)

El indicador de desempeño se conseguirá en base a los parámetros y matrices especificados en la Tabla 3.13.

INDICADOR DE DESEMPEÑO		
PARAMETRO		**MATRIZ**
1	Grado de Desempeño Real(d_r)	Matriz de Nivel de Servicio – Seguros del Pichincha
2	Grado de Desempeño COBIT(d_c)	

Tabla 3.13. Parámetros del Indicador de Desempeño
(COBIT 5, 2012)

El indicador de desempeño se alcanzara de los dos parámetros: desempeño real y desempeño COBIT, quedando la expresión como sigue:

$$d = \frac{d_r + d_c}{2}$$

Dónde: d_r=desempeño real, d_c=desempeño COBIT.

Modelo de medición de los objetivos de control

Como se vio anteriormente COBIT plantea 37 objetivos de gobierno generales, uno para cada proceso, y varios objetivos detallados para cada uno de ellos. El modelo de medición de los objetivos de gobierno evalúa el grado de efectividad y madurez de los objetivos de control detallados pertenecientes a cada proceso.

Indicador de Cumplimiento de los Objetivos (o)

El indicador de cumplimiento de los objetivos por proceso, se alcanzara valorando uno a uno de los objetivos detallados, logrando un parámetro único correspondiente al porcentaje de cumplimiento del objetivo de control. Ver Tabla 3.14.

INDICADOR DE CUMPLIMIENTO DE LOS OBJETIVOS		
PARAMETRO		**MATRIZ**
1	Grado de Cumplimiento de los objetivos de Gobierno Detallados(p)	Matriz Cumplimiento de Objetivos de Gobierno – COBIT

Tabla 3.14. Parámetros del Indicador de Cumplimiento de Objetivos
(COBIT 5, 2012)

Al emplear un solo parámetro para el cálculo de este indicador, la correspondencia es directa

$$o = p$$

MODELO DE IMPACTO

Este modelo implica tanto la importancia de un proceso dentro de Seguros del Pichincha como el impacto determinado por el marco de referencia COBIT para cada uno de ellos.

Una mezcla de estos dos parámetros aportará un impacto real de un determinado proceso dentro de TI.

Indicador de Impacto

Se calculará efectuando un promedio del Impacto de los procesos frente a los criterios de información de COBIT, con el valor de la importancia del proceso dentro de la institución, como lo muestra la Tabla 3.15.

INDICADOR DE IMPACTO		
PARAMETRO		**MATRIZ**
1	Grado de Impacto(I_C)	Matriz de Impactos de Procesos frente a los criterios de información de COBIT
2	Grado de Importancia(I_s)	Matriz de Diagnostico de Procesos – Seguros del Pichincha

Tabla 3.15. Parámetros del Indicador de Impacto
(COBIT 5, 2012)

$$I = \frac{I_c + I_S}{2}$$

Donde I=Impacto real, I_c=Impacto – COBIT,I_s=Importancia – Seguros del Pichincha

3.4.3.4 Descripción del Mapa de Relación COBIT – SEGUROS DEL PICHINCHA

El Mapa de Relación COBIT – SEGUROS DEL PICHINCHA permitirá relacionar las metas de la institución y metas TI, con los procesos y criterios de información de COBIT. Se aportara cinco planos basados en las directrices de COBIT 5, que contribuirán las equivalencias entre los procesos de TI de COBIT y las cinco áreas focales del gobierno de TI, los recursos de TI, las metas de TI y los criterios de información. Estos planos utilizarán la P cuando exista una relación primaria y la S cuando únicamente exista una relación secundaria. El hecho de que no exista una P ni una S no significa que no exista relación, sólo que es menos importante o marginal. COBIT 5 indica un mapeo entre estos mecanismos, sin embargo, recomienda que se examinen nuevamente estos mapas dentro de cada institución, razón por la cual, los planos serán desarrollados en la etapa de ejecución de la auditoría.

Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información

Esta matriz muestra las simetrías de las metas de la institución (Ver Tabla 3.7), de acuerdo al Balance Score card, con las metas de TI– COBIT (Ver Tabla 3.8) y con los criterios de información de COBIT. Esto ayuda a indicar, para una meta genérica de la institución, las metas de TI que por lo general dan soporte a esta meta, y los criterios de información de COBIT que se relacionan con la meta de la institución. Los criterios de información empleados fueron: efectividad, eficiencia, confidencialidad, integridad,

disponibilidad, cumplimiento y confiabilidad. La información lograda durante la ejecución de la auditoría sobre éste plano se encuentra en el: Anexo 5 - Tabla A5.1.

Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información

Señala los niveles de las metas de TI - COBIT (Ver Tabla 3.8) con los procesos de TI de COBIT, así como los criterios de información sobre los cuales se basa la meta de TI. Esta información se encuentra en el: Anexo 5 - Tabla A5.2.

Plano de Enlace de las metas TI y criterios de información

Proporciona un mapeo inverso que muestra para cada proceso de COBIT, las metas de TI – COBIT (Ver Tabla 3.8) que son soportadas. La información conseguida durante la ejecución de la auditoría sobre éste plano se encuentra en el: Anexo 5 - Tabla A5.4, Tabla A5.5.

Plano de Enlace de las metas corporativas de COBIT 5 y las metas relacionadas de TI

Este plano toma los procesos de TI listados en la Tabla 3.6, los relaciona con los criterios de información de COBIT (utilidad, usabilidad, credibilidad, libre de error, accesibilidad, conformidad y seguridad) y con las áreas de enfoque de gobierno de TI (alineación estratégica, entrega de valor, gestión de riesgos, gestión de recursos y medición del desempeño). La información alcanzada durante la ejecución de la auditoría sobre éste plano se encuentra en el: Anexo 5 - Tabla A5.5.

Plano de Responsabilidades de Procesos COBIT

Determina los responsables directos de cada proceso COBIT (Ver Tabla 3.6), de acuerdo al área encargada del proceso, en donde se incluyen los siguientes criterios:

Área Encargada del proceso Departamento de TI, Dentro de la Institución, Externo, No se sabe con certeza

La información lograda durante la ejecución de la auditoría sobre éste plano se encuentra en el: Anexo 5 - Tabla A5.6.

3.4.3.5 Descripción de las Matrices

Matriz de Grados de Madurez de Procesos – Seguros del Pichincha

El modelo de madurez para la administración y el control de los procesos de TI de acuerdo a COBIT se basa en un método de evaluación de la institución, en una escala simple que muestra como un proceso evoluciona desde una capacidad no existente (0),

hasta una capacidad optimizada (5).El modelo genérico de madurez propuesto por COBIT se muestra en la Tabla 3.16

El modelo de madurez a emplear para la auditoría informática a Seguros del Pichincha, tomará los principios de COBIT. Una evaluación de la madurez bajo COBIT resultará en un perfil donde condiciones relevantes a diferentes niveles de madurez se han adquirido, es decir algunos procesos estarán en diferentes grados de madurez de acuerdo a como se han completado los objetivos, metas y actividades proporcionados a dicho proceso

MODELO GENERICO DE MADUREZ COBIT		
0	Incompleto	Carencia completa de cualquier proceso reconocible. La institución no ha reconocido siquiera que existe un problema a resolver.
1	Alcanzado	Existe evidencia que la institución ha reconocido que los problemas existen y requieran ser resueltos. Sim embargo; no existen procesos estándar en su lugar existen enfoques que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2	Gestionado	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad del individuo. Existe un alto grado de confianza en el conocimiento de los individuos y por tanto los errores son más probables
3	Establecido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en si no son sofisticados pero formalizan las prácticas existentes.
4	Predecible	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada
5	Optimizado	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y un modelo de madurez con otras instituciones. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y efectividad, haciendo que la institución se adapte de manera rápida.

Tabla 3.16. Modelo Genérico de Madurez – COBIT.
(COBIT, 2012)

Las equivalencias porcentuales para cada nivel se obtendrán de la siguiente manera:

$$V_i = \frac{100}{N_i} n_i$$

Dónde:

$v_i = valor\ porcentual\ del\ nivel\ i$

$N_i = numero\ total\ de\ caracteristicas\ consideradas\ en\ el\ nivel\ i$

$n_i = numero\ de\ caracteristicas\ que\ se\ cumplen\ en\ el\ nivel\ i$

Los datos serán plasmados en una tabla que guarde un control de niveles por cada proceso. El nivel de madurez logrado corresponderá a aquel nivel que tenga el mayor grado de madurez calculado. Esto es debido a que cada una de las características de los niveles detallan el cumplimiento de hechos que sitúan a un proceso en determinado nivel.

$$m_r = Mayor(v_0, v_1, v_2, v_3, v_4, v_5)$$

$$n_r \leftrightarrow m_r$$

Donde m_r= Grado de Madurez Real, $v_0, v_1, v_2, v_3, v_4, v_5$ = Valores porcentuales de los niveles del 0 – 5 respectivamente, n_r= Nivel de Madurez Real

Los resultados alcanzados de cada proceso se resumirán en una Matriz de Grados de Madurez de Procesos – Seguros del Pichincha que alcanzara el grado y nivel de madurez para cada proceso COBIT. La información lograda durante la ejecución de la auditoría para esta matriz se encuentra en el: Anexo 5 - Tabla A5.7.

Matriz de Nivel de Servicio – Seguros del Pichincha

Evalúa el desempeño de cada uno de los procesos COBIT, de acuerdo al siguiente criterio:

Desempeño Nivel de resultados que se están logrando en las actividades realizadas

El parámetro desempeño es utilizado para el cálculo del indicador del mismo nombre, para lo cual se utilizarán las equivalencias cuantitativas mostradas en la Tabla 3.17

EQUIVALENCIAS DE DESEMPEÑO		
DESEMPEÑO		**CUMPLIMIENTO DE OBJETIVOS COBIT GENERALES**
No existe	0	No cumple
Deficiente	1 – 20	Cumple Levemente
Regular	21 – 40	Cumple Parcialmente
Satisfactorio	41 – 60	Cumple Mayoritariamente
Muy bueno	61 – 80	Cumple casi totalmente
Excelente	81 – 100	Cumple Totalmente

Tabla 3.17. Equivalencias de Desempeño
(COBIT 5, 2012)

La información conseguida durante la ejecución de la auditoría para ésta matriz se encuentra en el: Anexo 5 - Tabla A5.8.

Para las encuestas a los usuarios se manejará una descripción del proceso y se evaluará su nivel de cumplimiento, para que exista un mejor entendimiento de los encuestados. Los resultados serán tabulados empleando las equivalencias correspondientes.

Matriz de Cumplimiento de Objetivos de Control – COBIT

COBIT plantea una cadena de objetivos de control para cada uno de los 37 procesos listados en la Tabla 3.6. Durante la realización de la auditoría se determinó el cumplimiento de cada objetivo de control, esto se muestra en la Tabla A5.9 del Anexo 5.

Matriz de Impacto de Procesos frente a los criterios de información de COBIT

Esta matriz corresponde al impacto de los procesos frente a los siete criterios de información y recursos de TI bajo COBIT.

La relación cualitativa utilizada en los criterios de información para esta tabla será la que se expuso anteriormente en la Tabla 3.14. Sin embargo se hará una correspondencia cuantitativa para obtener los porcentajes de los criterios de información o el porcentaje de utilidad, usabilidad, seguridad, libre de error, accesibilidad, conformidad y credibilidad. Se asignará un valor al grado de impacto Primario cuyo efecto es alto o fuerte, Secundario cuyo efecto es leve o medio. Este porcentaje se determina en base a una propuesta metodológica establecida por una metodología de manejo de riesgos como es COSO.

COSO (Sponsoring Organizations of the Treadway) constituye una ponderación para el grado de impacto que tienen los criterios de información dentro de un proceso, además de acceder a determinar el nivel de riesgo que tendría dicho proceso, para lo cual establece rangos de calificación para los niveles bajo, medio alto; como se puede apreciar en la Tabla 3.18.

INTERPRETACION DE IMPACTOS – COSO	
IMPACTO	**RANGO DE CALIFICACION**
Bajo	15%-50%
Medio	51%-75%
Alto	76%-95%
Vacío	-

Tabla 3.18. Interpretación de los Impactos de acuerdo a COSO (COBIT 5, 2012)

Tomando en cuenta la propuesta de COSO se ha generado una tabla de ponderaciones mediante la cual se plantea asignar un valor numérico al impacto de los criterios de

información de cada proceso, para esto se ha determinado tomar el valor promedio de cada uno de los rangos, eliminando así la subjetividad el momento en que se asigna un valor numérico al impacto, dando como resultado la Tabla 3.19.

EQUIVALENCIAS DEL IMPACTO	
IMPACTO	**PROMEDIO**
Bajo	32%
Medio	63%
Alto	86%

Tabla 3.19. Equivalencias del Impacto
(COBIT 5, 2012)

A continuación se plantarán los valores obtenidos en los criterios de Información que establece COBIT, dentro de cada uno de los procesos, para el grado de impacto Primario se asigna el 86%, cuyo impacto es alto, para el grado secundario se asigna el 63% cuyo impacto es medio, para el grado terciario se asigna 32% cuyo impacto es bajo y para el caso en que la casilla se encuentre en blanco (vació), no se asignara ningún valor, ya que no impacta en nada a los criterios de información, según lo que especifica COBIT. Finalmente una vez que se han determinado los valores a cada uno de los Criterios de información se procederá a utilizarlos en el cálculo del porcentaje de impacto, en donde intervendrán los criterios de efectividad y eficiencia. El porcentaje del impacto estará dado por el promedio del impacto de estos dos criterios de información

$$I = i_e + i_i$$

Donde I =Impacto, i_e =Impacto de la efectividad, i_i= impacto de la eficiencia

La matriz de impacto de procesos, además de acordar un indicador numérico para cada criterio de información de COBIT y un porcentaje de impacto global, señalara una relación con los recursos de TI empleados, considerando: personas, información, aplicaciones e infraestructura.

Matriz de Diagnóstico de Procesos COBIT

Proporcionará determinar la importancia, el fundamento y los controles que se están realizando en cada uno de los procesos, de acuerdo a los siguientes criterios:

Importancia	Nivel de transcendencia de los procesos. (Poco importante, importante, Muy importante)
Formalizado	Se refiere a si existe algún documento que norme la forma de realizar la actividad consultada (No Formalizado, Formalizado, No, No Aplica, No se sabe con certeza)
Control Interno	Se refiere a la documentación formal aprobada y difundida en la institución sobre las actividades realizadas y consultadas. (No Documentado, Documentado, No se sabe con certeza)
Auditado	(No Auditado, Auditado, No se sabe con certeza)

El parámetro de importancia se maneja en el cálculo del indicador de impacto para lo cual se emplean las equivalencias mostradas en la Tabla 3.20

EQUIVALENCIAS DE IMPORTANCIA	
Poco Importante	33%
Importante	67%
Muy Importante	100%

Tabla 3.20. Equivalencias Cuantitativas de la Importancia (COBIT 5, 2012)

La información de esta matriz desarrollada durante el proceso de auditoría se encuentra en el: Anexo 5, Tabla A5.10.

3.4.3.6 Determinación de Resultados y Productos de la Auditoría

Los resultados de la auditoría informática a Seguros del Pichincha se verán presentados en el informe final y la carta de presentación, los mismos que exhibirán el análisis de cada uno de los procesos basados en los productos obtenidos durante la ejecución de la auditoría.

Productos de la Auditoria

Los productos de la auditoría informática, se agrupan en dos ámbitos conceptuales, planos y matrices, los primeros reconocerán establecer las relaciones entre los procesos pertenecientes a la metodología aplicada COBIT y los procesos de Seguros del Pichincha. Las matrices en cambio muestran indicadores cualitativos y/o cuantitativos

que reflejan una situación sobre cada proceso u objetivo de gobierno de COBIT. Un resumen se muestra en la Figura 3.3.

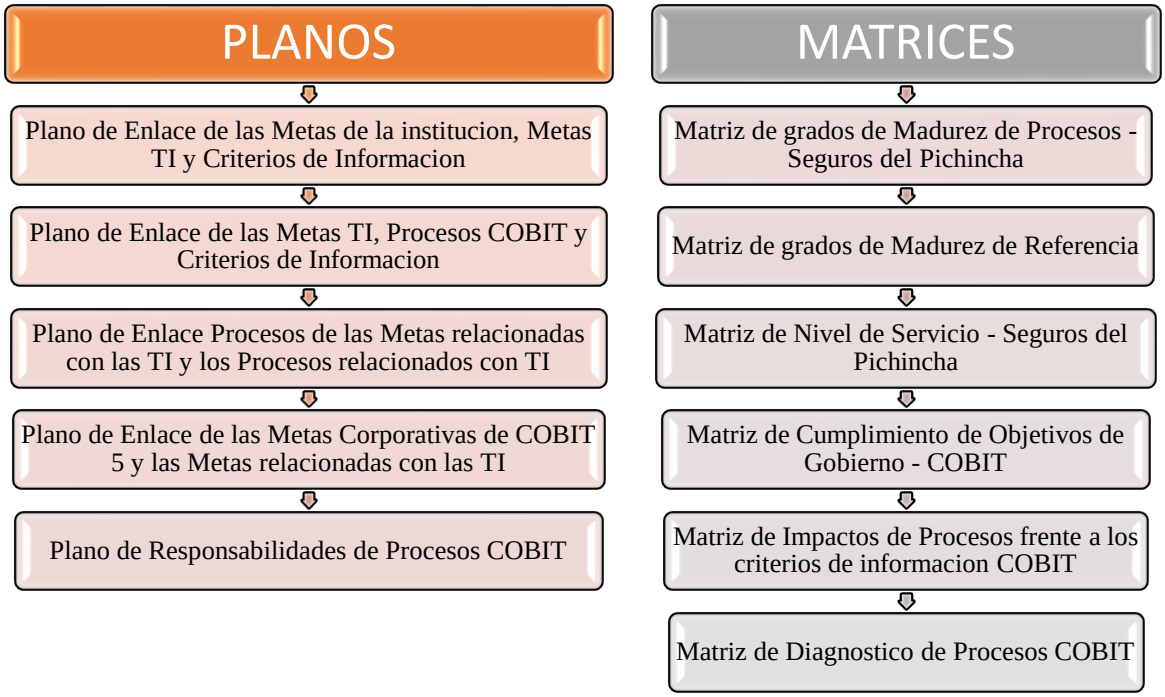


Figura 3.3. Productos de Auditoria Informática para Seguros del Pichincha
Elaborado por el Autor

Resultados

Los resultados de la auditoría se verán plasmados en los dos únicos documentos entregables, el informe final y la carta de presentación, los cuales serán los únicos elementos constatables de la realización de la auditoría. Ver Figura 3.4. El informe final especificará de manera detallada el análisis, resultados, recomendaciones e indicadores obtenidos para cada uno de los procesos COBIT. La carta de presentación llevará un resumen del informe de auditoría.

Figura 3.4. Resultados de Auditoria Informática para Seguros del Pichincha
Elaborado por el Autor

3.4.3.7 Recursos para la auditoría

Una de las partes más importantes dentro de la coordinación de la auditoria en informática es el personal que deberá participar. Uno de las representaciones generalmente aceptados para tener un grupo adecuado que interceda en el proceso, es que esté debidamente capacitado, tenga disponibilidad y un alto sentido de honradez, que pueda proveer toda la información que se solicite, coordinar las reuniones y entrevistas requeridas. Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas. También se debe contar con personas fijadas a nivel de usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se está solicitando, y complementen el grupo multidisciplinario; ya no sólo se examinará el punto de vista de la dirección de informática, sino también el de los usuarios. Se establecen tres categorías para la realización de la auditoría:

Responsable de la auditoría: Realizara las tareas de organización de actividades con la empresa, de obtención de las facilidades para el acceso a la información y la documentación de soporte para toda la auditoría. Sr. Patricio Auquilla

Auditor: Cumplirá con las tareas de colección, recopilación, categorización, y análisis de la información. Deberá tener conocimiento de la metodología COBIT y su aplicación. Sr. Patricio Auquilla Chavez

Auditados: Brindarán la información requerida y coordinarán actividades que se requieran para el cumplimiento del plan y programa de auditoría. La selección de la muestra de auditados se realizará a continuación

Selección de la Muestra de Auditados

Para la ejecución de la auditoría al Departamento de TI de Seguros del Pichincha, se procederá con la selección de un grupo de personas que concedan los datos que reflejen las vivencias del encuestado en sus áreas de trabajo. Ver Figura 3.4.

De acuerdo al número de empleados de Seguros del Pichincha que son 200, es necesario aplicar una teoría de muestreo con enfoque matemático para la tabulación, se usará una selección de la muestra especificada a partir de la población seleccionada.

$$n_0 = (\frac{Z}{\in})^2 * p * q$$

$$n = \frac{n_0}{1 + \frac{n_0}{N}}$$

Dónde:

n_0: Cantidad teorica de elementos de la muestra.

n: Cantidad real de elementos de la muestra a partir de la población asumida

N: Número total de elementos que conforman la población. N=200

z: Valor estandarizado en función del grado de confiabilidad de la muestra calculada. Para una confiabilidad de 95%, z=1.96

$\in$: Error asumido en el cálculo. Para N > 10. Se asume $\in$=0.05 (un error del 5%).

q: Probabilidad de la población que no presenta las características universales. Para N≥80. Se asume q=0.05 – 0.20. (5 al 20 %). Se asumirá un valor de 5% debido a que ya se ha excluido de la población a funcionarios auxiliares que no aportarían en la determinación de resultados (ayudantes de oficina, conductores, entre otros). La

probalidad de que la población considerada no represente las características comunes será la mínima recomendada.

p: Probalidad de la población que presenta las características universales

$$p = 1 - q = 1 - 0.05 = 0.95$$

De acuerdo los parámetros especificados. Se calculara el tamaño de la muestra, quedando como sigue

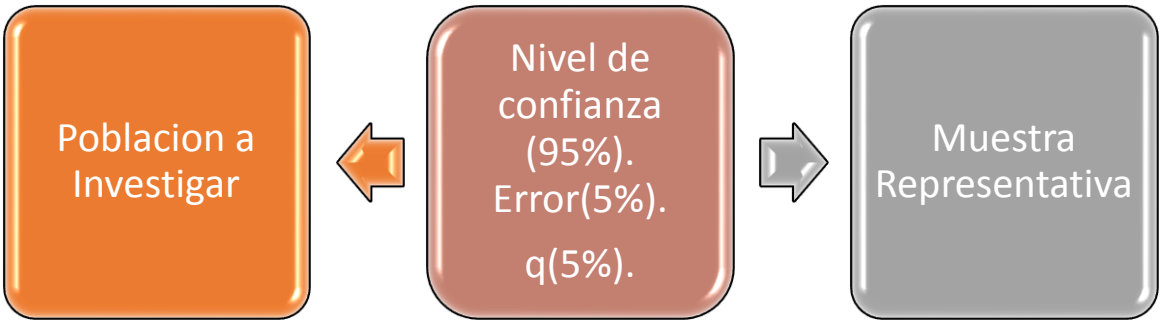


Figura 3.5. Selección de la Muestra de Auditados
Elaborado por el Autor

$$n_0 = (\frac{Z}{\epsilon})^2 * p * q = \left(\frac{1.96}{0.05}\right)^2 * 0.95 * 0.05 = 72.99$$

$$n = \frac{n_0}{1 + \frac{n_0}{N}} = \frac{72.99}{1 + \frac{72.99}{85}} = 39{,}45 \sim 40$$

El tamaño de la muestra calculado corresponde a 40 personas que participaran en la encuesta, teniendo una población de 160 usuarios de tecnología de información, que forman parte de un total de 200 funcionarios de Seguros del Pichincha. La muestra corresponde al 21.89% de la población. La Tabla 3.22 detalla el tamaño de las muestras por cada grupo definido por COBIT y de acuerdo a las áreas de Seguros del Pichincha. Los grupos considerados y sugeridos por COBIT, son:

DIRECTORIO: Para conocer la opinión de cuáles son los temas de mayor interés a nivel de autoridades y directivos

DEPARTAMENTO DE TI: Constituye el ente que está siendo evaluado, por lo tanto es importante la opinión de ellos en las prioridades de la información recopilada

USUARIOS: Proporcionan las pautas para evaluar el funcionamiento de sistemas, procesos, servicios y equipos de TI.

SELECCIÓN DE LA MUESTRA			
GRUPOS	**PARTICIPANTES**	**POBLACION**	**MUESTRA**
DIRECTORIO	Directivos	10	6
TECNOLOGIA DE LA INFORMACION	Informáticos	20	5
USUARIOS	Administrativos	60	11
	Técnicos	20	10
	Jurídicos	25	5
	Financiero	25	3
TOTAL MUESTRA		160	40
OTROS		40	0
TOTAL FUNCIONARIOS		200	

Tabla 3.21. Selección de la muestra.
Elaborado por el Autor

Con esto estamos indicando que 40 usuarios serán encuestados bajo diferentes cuestionarios, lo que definirá las prioridades y la profundidad con la que se tratarán los procesos del marco de referencia COBIT sujetos a la auditoría. Antes de empezar a procesar los datos se ha preparado a los funcionarios y a los directivos para describir lo que implica aplicar la metodología COBIT en la institución, qué beneficios se pueden obtener, cuáles son las áreas en las cuales se enfocará el estudio y cuál es el proceso que se seguirá. De acuerdo a la planificación, la auditoría empleará cuestionarios, entrevistas, recopilación de información, y análisis de la misma. Por lo tanto se requerirá lo siguiente:

Hardware: Computador de características generales, para la documentación y almacenamiento de resultados y actividades desarrolladas en el proceso de auditoría.
Software: Los programas que servirán de apoyo para este proyecto de auditoría son los siguientes: procesadores de texto, hojas de cálculo, herramientas para generación y edición de gráficos, browsers.

3.4.3.8 Programa de auditoría

El programa de auditoria constituye un elemento metodológico que encaminara el proceso de análisis y determinación de cada uno de los parámetros que se evalúan dentro de los modelos contemplados en la estrategia. La aplicación de los Modelos basados en los procesos y objetivos de gobiernos propuestos por COBIT, establecerán cubrir políticas, planes y procesos en el área de tecnologías de la información TI, así como también el desempeño de equipos y sistemas, la satisfacción de los usuarios y el alineamiento con los objetivos estratégicos de la institución. El Programa planteado se detalla en la Tabla 3.22

PROGRAMA DE AUDITORIA		
MODELO	**PRODUCTO**	**TECNICA**
Mapa de Relación COBIT-Seguros del Pichincha	Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información	Se obtiene del análisis de la información de Seguros del Pichincha, observaciones, indagación, entrevistas y encuestas para recabar información
	Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información	
	Plano de Enlace Procesos de COBIT a Metas de TI	
	Plano de Enlace de Procesos COBIT a Gobierno de TI y Criterios de Información	
	Plano de Responsabilidades de Procesos COBIT	
Modelo de Madurez	Matriz de Grados de Madurez de Procesos – Seguros del Pichincha	Se obtiene del análisis la información, observaciones, entrevistas y encuestas realizadas para recabar información
	Matriz de Grados de Madurez de Referencia	Obtenida del nivel de exigencia de los usuarios de TI de Seguros del Pichincha
Modelo de Desempeño	Matriz de Nivel de Servicio – Seguros del Pichincha	Obtenida mediante encuestas
	Matriz de Evaluación de Procesos bajo Métricas COBIT	Obtenida mediante mediciones, evaluaciones, observaciones y análisis
Modelo de Cumplimiento de Objetivos	Matriz de Cumplimiento de Objetivos de Gobierno – COBIT	Obtenida del análisis y observación del cumplimiento y desempeño de cada objetivo de control detallado.
Modelo de Impactos	Matriz de Impactos de Procesos frente a los criterios de información de COBIT	Marco de Referencia COBIT aplicado a Seguros del Pichincha
	Matriz de Diagnostico de Procesos COBIT	Se obtiene mediante encuestas y análisis de información.

Tabla 3.22. Programa de Auditoria
Elaborado por el Autor

3.4.3.9 Cronograma de actividades para la Auditoría

El control del avance de la auditoria es esencial para el resultado eficiente de la misma por lo que se ha realizado un cronograma de ejecución que define las tareas y tiempos asignados para su cumplimiento, lo cual proporcionará el alcance a los procedimientos de control así como también permitirá asegurarse de que el trabajo se está llevando a cabo de acuerdo con el programa de auditoria, con los recursos estimados y en el tiempo señalado en la planeación. En la Tabla 3.23 se detalla toda la planificación de la auditoría.

CRONOGRAMA DE ACTIVIDADES	
TAREA	**TIEMPO**
AUDITORIA SEGUROS DEL PICHINCHA	**Días**
ESTUDIO PRELIMINAR	**15**
Solicitud de la Información	3
Recopilación de la Información	2
Ordenamiento de la Información	1
Elaboración de Cuestionarios	4
Realización de Encuestas y Entrevistas	5
PLANEACION DE LA AUDITORIA	**20**
Comprensión del Control Interno	3
Desarrollo de la estrategia de Auditoria	5
Determinación de los resultados y productos de la auditoria	2
Determinación de los recursos necesarios para realizar la auditoria de sistemas	5
Elaboración los Programas de Trabajo	3
Cronograma	2
EJECUCION DE LA AUDITORIA	**27**
Entrevista a líderes y usuarios más relevantes de la dirección de TI	3
Entrevistas y encuestas a usuarios	3
Determinación del Mapa Relación COBIT – Seguros del Pichincha	3
Ejecución de los Modelos de Madurez, Desempeño, Impacto y Riesgo	3
Evaluación y análisis del dominio evaluar, orientar y supervisar	3
Evaluación y análisis del dominio alinear, planificar y organizar	3
Evaluación y análisis del dominio cconstruir, adquirir e implementar	3
Evaluación y análisis del dominio eentregar, dar servicio y soporte	3
Evaluación y análisis del dominio ssupervisar, evaluar y valorar	3
INFORME FINAL	**10**
Revisión de los papeles de trabajo	4
Elaboración de Informe	4
Elaboración de la carta de presentación	2
TOTAL	**72**

Tabla 3.23 Cronograma de Auditoria
Elaborado por El Autor

3.5 Informe de Auditoría

En el desarrollo del presente capítulo se encuentra detallada la carta de presentación, que forma parte del "Informe Final" y corresponde a la última fase de la auditoría. La carta de presentación muestra resultados globales de los 37 procesos COBIT que intervinieron durante la ejecución de la Auditoria Informática, sin embargo un detalle de los resultados e indicadores para cada uno de los procesos se encuentra en el Anexo 5.

3.5.1 Carta de Presentación de la Auditoría Informática

En Seguros del Pichincha, una aseguradora con visión a ser la mejor Aseguradora en el País apoyando el desarrollo del país siendo una empresa sin fines de lucro; cuenta con una infraestructura tecnológica muy extensa para solventar dichas tareas, y se soporta en el manejo de información que atiende cada uno de los procesos que forman parte del Modelo de Gestión por Procesos Institucional, a través del Departamento de Tecnología de Información. La auditoría informática ha permitido evaluar el uso de la tecnología de

la información en los procesos institucionales, y determinar indicadores de la situación actual, analizar tendencias, puntos débiles y amenazas, para emitir recomendaciones que permitan mantener una optimización constante de las tecnologías de la información en la institución.

El proceso de auditoría se desarrolló bajo el marco de referencia COBIT (Control Objectives for Information and related Tecnology) por ser un estándar que asocia las mejores prácticas para el control de TI y para la implementación de Gobierno de TI; ya que permite asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgos institucionales. Estas características lo han posicionado como uno de los modelos más utilizados en el mundo, por usuarios, directivos y auditores.

Los temas que han sido objeto de la auditoría corresponden a treinta y siete procesos COBIT, que cubren todos los aspectos involucrados en Tecnología de la información y se agrupan en cinco categorías: EVALUAR, ORIENTAR Y SUPERVISAR (EDM), ALINEAR, PLANIFICAR Y ORGANIZAR (APO), CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI), ENTREGAR, DAR SERVICIO Y SOPORTE (DSS), SUPERVISAR, EVALUAR Y VALORAR (MEA).

La auditoría ha atendido estos temas a través de un conjunto de matrices que registran indicadores cualitativos y cuantitativos resultantes de la aplicación de modelos, y mediciones, que a su vez emplean para su construcción, diversas técnicas de auditoría como observaciones, entrevistas, indagaciones, entre otros. Los modelos, planos y matrices empleados durante la ejecución de la auditoría han sido los siguientes:

Modelos de madurez, que han permitido determinar la situación actual de los procesos de TI e identificar las mejoras necesarias. Interviene:
Matriz de Grados de Madurez de Procesos – Seguros del Pichincha

Metas y mediciones de desempeño para los procesos de TI, que han permitido evaluar cómo los procesos satisfacen las necesidades de Seguros del Pichincha y de TI. Intervienen las siguientes matrices:
Matriz de Nivel de Servicio – Seguros del Pichincha. Parámetro Desempeño
Matriz de Evaluación de Procesos bajo Métricas COBIT

Mediciones de objetivos de control de manera que determinen el estado real de la ejecución de los procesos para facilitar su desempeño. Interviene la siguiente matriz:
Matriz de Cumplimiento de Objetivos de Gobierno – COBIT

Determinación del nivel de impacto de cada uno de los procesos en la institución. Intervienen las siguientes matrices:
Matriz de Impactos de Procesos frente a los criterios de información de COBIT.
Matriz de Diagnóstico de Procesos COBIT

Con el fin de enlazar los procesos de tecnologías de información estándares planteados por COBIT con los procesos de TI institucionales, se desarrolló un MAPA DE RELACIÓN COBIT-Seguros del Pichincha, el cual está conformado por cinco planos:
Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información
Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información
Plano de Enlace Procesos de COBIT a Metas de TI
Plano de Enlace de Procesos COBIT a Gobierno de TI y Criterios de Información
Plano de Responsabilidades de Procesos COBIT

Análisis de Servicios y Productos ofrecidos por la Tecnologías de la Información de Seguros del Pichincha
Los Servicios y Productos ofrecidos por las TI, se encuentran identificados en el Catálogo de Servicios de Seguros del Pichincha de la tabla 3.24.En donde se ha tratado de resumir y agrupar servicios a fines o con características similares; esto se debe a que el catalogo original detalla servicios de acuerdo a los aplicativos existentes, que en muchos casos son soluciones de legado, aisladas y con tecnologías distintas como resultado de las varias modificaciones organizativas y estructurales que ha sufrido la empresa en el transcurso del tiempo.(Quintuña, Veronica, 2012).

FAMILIA DE SERVICIOS CORPORATIVOS			
SERVICIO	**DESCRIPCION DEL SERVICIO**	**AREA RESPONSABLE**	**OBSERVACIONES**
Equipos de cómputo de oficina	Mantenimiento de equipos de escritorio, portátiles, escaners, impresoras, proyectores, entre otros.	Soporte a Usuarios(investigar)	El mantenimiento de impresoras lo realiza el proveedor Fesa Ecuador()
Aplicaciones de escritorio	Instalación, actualización y configuración de los programas y utilitarios empresariales	Soporte a usuarios	Incluye: antivirus, clientes de correo, aplicaciones ofimáticas, entre otras.
Impresión	Impresión de boletines, certificados, etc. relacionados de Seguros del Pichincha	FesaEcuador	
Correo electrónico	Sistema para intercambio de información por vía electrónica, a través de las aplicaciones cliente o el portal web	Soporte a usuarios	Se considera dentro de este servicio, la emisión de comunicados corporativos y boletines electrónicos.
Alojamiento WEB	Brinda almacenamiento y pone a disposición de los usuarios material multimedia, aplicaciones, archivos, entre otros.	Senior de Datos Senior de Aplicaciones	Este servicio está disponible para todos los servicios y aplicaciones propias de Seguros del Pichincha, desplegadas en intranet e internet
Servicios de Internet	Es el conjunto de redes interconectadas, internas y externas, que da soporte a protocolos para transmisión e intercambio de imágenes, archivos, telefonía, correo electrónico etc.	Soporte a usuarios, TE UNO	El mantenimiento correctivo y preventivo de la red está a cargo del Proveedor TeUno
Telefonía	Es el servicio telefónico como tal	Infraestructura y comunicación	
Video Conferencia	Comunicación multimedia en tiempo real, para la realización de reuniones desde múltiple servicios remotos de forma simultanea	Soporte a usuarios	
Data Warehouse/Data	Mantenimiento de los repositorios de información y los programas de inteligencia de negocios	Senior de Datos Senior de Aplicaciones	
Gestión Documental	Gestión de contenido y flujos de trabajo	Senior de Aplicaciones	
Aplicaciones complementarias	Desarrollo,soporte,mantenimiento de múltiples aplicaciones que complementan los sistemas corporativos o atienden necesidades puntuales de las áreas de la empresa	Senior de aplicaciones	Incluye los siguientes aplicativos: Agenda, control de asistencia, control de bodega, control de gastos médicos, control de pólizas y seguros, registro de proveedores, auditoría y control, órdenes de pago, sistema para acceso a documentos, viáticos.

Tabla 3.24. Catálogo de Servicios
Elaborado de Seguros del Pichincha

Análisis de la Seguridad de la información de Seguros del Pichincha

Análisis de los informes de Hacking ético

Seguros del Pichincha, como parte de las iniciativas de modernización tecnológica que se está ejecutando, contrato en el año 2013 los servicios de consultoría para la realización de pruebas de Hacking Ético[2]en la infraestructura tecnológica de la empresa. Los objetivos principales de la consultoría fueron los siguientes:

- Identificar riesgos potenciales de seguridad informática y oportunidades de mejora
- Identificar potenciales problemas de seguridad, fraudes o fugas de información que pueden encontrarse en el personal o elementos tecnológicos
- Priorizar un plan de acción de acuerdo al nivel de impacto de los riegos identificados
- Establecer recomendaciones, de acuerdo a las buenas prácticas de seguridad, para mitigar los riesgos identificados.

Equipos utilizados para las pruebas de Hacking ético

Los equipos utilizados para las pruebas de Hacking ético comprenden computadores portátiles con software de virtualización para la ejecución de distribución Windows. Las distribuciones Windows son sistemas operativos a los cuales se les ha instalado y configurado un conjunto de herramientas de software que han sido desarrolladas y seleccionadas por profesionales en seguridad. Las herramientas que normalmente son incluidas en estas distribuciones se clasifican, según la funcionalidad en los siguientes grupos:

- Recolección de información
- Evaluación de vulnerabilidades
- Herramientas de explotación
- Escalamiento de Privilegios
- Mantenimiento o persistencia de acceso
- Ingeniería inversa

[2] HACKIN ETICO: Actividad realizada por un experto que conoce y entiende las vulnerabilidades de los sistemas informáticos, que tiene como objetivo realizar pruebas de penetración con herramientas y técnicas similares a las usadas por intrusos o hackers

- Pruebas de estrés
- Informática Forense

Resultados de las pruebas externas de Hacking Ético de Seguros del Pichincha

Las pruebas externas fueron realizadas sobre los siguientes dominios públicos

DOMINIO	GERENCIA/UBICACIÓN
seg-pichincha.com	Gerencia General, Matriz

Tabla 3.25. Dominio para pruebas de Hacking Ético Externo
Elaborado por el autor

El número de equipos analizados, dentro de los dominios ates detallados, fue de 23, de los cuales el 39% se encuentra afectado por vulnerabilidades, como se detalla en la Figura 3.6.

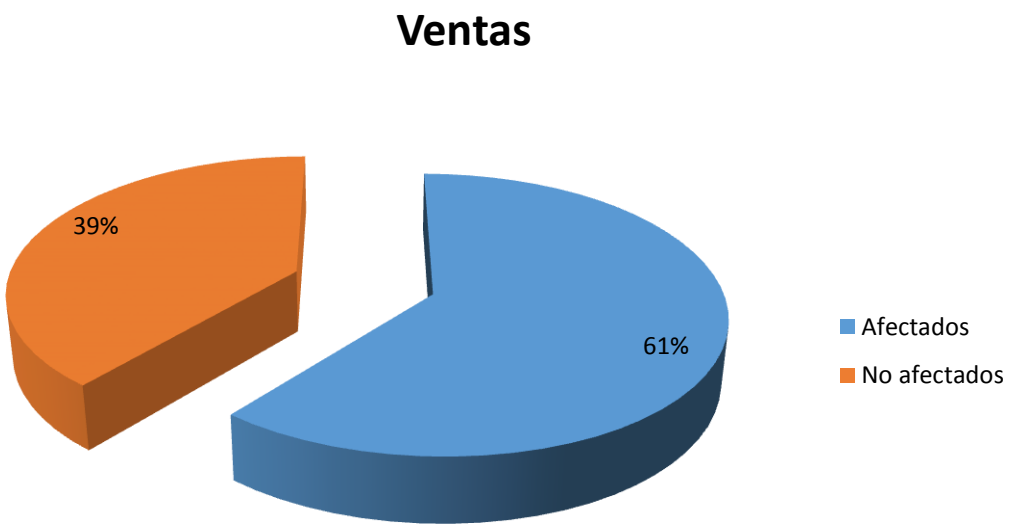


Figura 3.6. Equipos externos afectados por vulnerabilidades
Elaborado por el Autor

Las vulnerabilidades detectadas en la infraestructura externa de Seguros del Pichincha se resumen en la siguiente tabla 3.26:

Vulnerabilidad	Equipos Afectados	CVE[3]	Descripción de la vulnerabilidad
Inyección SQL Blind	1	OWASP-DV-005	Permite realizar consultas sobre el servidor de base de datos utilizando la interfaz de la aplicación, de esta manera un atacante puede obtener información de retorno de los objetos y tablas existentes
Stored Cross Site Scripting (XSS)	1	OWASP-DV-002	Ocurre cuando una aplicación web solicita información y la almacena para un uso posterior, si esta información no es filtrada, un atacante puede ingresar código malicioso que luego puede ser ejecutado como parte de la aplicación web
Servicio FTP con usuario anonymous habilitado	2	1999-0497	Permite ingresar al servidor FTP sin utilizar credenciales de autentificación, exponiendo la información empresarial que se encuentre en este servidor, o permitiendo la carga de exploits.[4]
Usuarios y Contraseñas débiles	2	N/A	Las contraseñas o claves utilizadas para la validación en las consolas de administración de las aplicaciones utilizan palabras comunes y pueden ser susceptibles a ataques
Acceso a configuración del servidor mediante componente instalado en el mismo	1	N/A	Las aplicaciones web exponen componentes que pueden ejecutar código de configuración. Estos componentes normalmente no están disponibles en un ambiente de producción.
Servicio SMTP relay habilitado	2	CVE-1999-0512 CVE-2002-1278 CVE-2003-0285	Los servidores SMTP[5] permiten él envió de correos mediante línea de comandos, de esta manera un atacante puede suplantar la identidad del remitente para obtener información, transmitir información falsa, generar eventos inmorales, entre otros.
Consolas de acceso permiten acceder a información privada o confidencial	1	OWASP-CM-007	Las aplicaciones web exponen sus consolas de administración sin filtrado de direcciones IP o con autentificación débil.
Divulgación de información a través de archivos no referenciados	1	OWASP-CM-006	Algunas aplicaciones web permiten la indexación de directorios, de esta manera se puede obtener gran cantidad de archivos y los metadatos asociados. Son fuente de información para ataques más elaborados.
Directorio de publicación de scripts y código fuente PHP	1	OWASP-CM-004	Las aplicaciones exponen directorios con código fuente y archivos de configuración de las aplicaciones, lo cual permite obtener información de otros equipos de la red interna
Archivo Robots.txt se encuentra habilitado en el sitio web	1	N/A	Los sitios web tiene habilitado el archivo robots.text, que se utiliza para la indexación de páginas a través de buscadores. Puede proveer a un atacante, la ruta de los directorios que contiene el sitio, facilitando la búsqueda de archivos que brinden información sobre configuración.
Puntos de acceso/login web podrían permitir la intercepción de información en texto claro	1	N/A	Las páginas de login o autentificación no utilizan un protocolo seguro que cifre la comunicación entre el cliente y el servidor. La información de usuario y contraseña viajan por la red en texto plano y podrían ser recuperados por un atacante que se encuentre analizando el tráfico de red.
Métodos tipo TRACE habilitados en el servidor	1	CVE-2003-1567 CVE-2004-2320 CVE-2010-0386	Los servidores tienen habilitados los métodos de tipo HTTP TRACE, mediante la cual un atacante podría extraer información sensible respecto a la configuración del servidor o información relacionada con las sesiones de los usuarios conectados.

Tabla 3.26. Vulnerabilidades Seguros del Pichincha para pruebas externas
Elaborado por el Autor

[3] CVE: Vulnerabilidades y Exposiciones Comunes, Common Vulnerabilities and Exposures por sus siglas en ingles. Es un diccionario de nombres comunes para las vulnerabilidades de seguridad de información de conocimiento público.

[4] EXPLOIT: Es un fragmento de código o conjunto de comandos que se utiliza para aprovechar una vulnerabilidad de seguridad de un sistema de información, logrando que este se comporte de una manera determinada

[5] SMTP: Protocolo simple para transferencia de correo, Simple Mail Tranfer Protocol por sus siglas en Ingles

Resultados de las pruebas internas de Hacking Ético de Seguros del Pichincha

Las pruebas internas fueron realizadas sobre los siguientes objetivos de análisis:

Tipo	Características	Tipo de Pruebas
Segmentos de Red	Edificio AutoDelta(Quito)	Escaneo de puerto, explotación de vulnerabilidades, suplantación y captura de trafico Wireless, monitoreo de tráfico, envenenamiento ARP
	Edificio Coruña(Quito)	
	Edificio Banco Pichincha(Guayaquil)	
	Edificio Portoviejo(Portoviejo)	
Servidores	Servidores distribuidos en 3 VLAN[6]	Inyección SQL y mal formación de parámetros, cross site scripting, escaneo de puertos, análisis de código fuente generado(HTML, JavaScript), manipulación de controles, data fuzzing[7]
Dominios	3 controladores de dominio	Envenenamiento ARP, ataques de hombre en el medio, explotación de vulnerabilidades
Computadores personales	Varios equipo seleccionados aleatoriamente	Ataques de fuerza bruta, ataque de hombre en el medio, pruebas de obtención de huellas

Tabla 3.27. Objetivos de análisis para pruebas internas de Hacking Ético
Elaborado por el Autor

[6] VLAN: Red de área local virtual. Virtual Local Area Network, por sus siglas en ingles
[7] DATA FUZZING:Tecnica que consiste en proporcionar a los sistemas y aplicaciones información incorrecta, incompleta o aleatoria con el objetivo de detectar vulnerabilidades o fallas de pérdida de memoria

Las vulnerabilidades detectadas en la infraestructura interna de Seguros del Pichincha se resumen en la siguiente tabla:

Vulnerabilidad	Equipos afectados	CVE	Descripción de la vulnerabilidad
Enumeración de servicios y versiones	376	N/A	Los equipos probados entregan fácilmente información que permite identificar, sistema operativo, versiones, servicios. Esta información permite planificar un ataque más elaborado
Protocolo de cifrado débil SSL	49	N/A	La versión de SSL usadas en algunos servidores es antigua y se considera obsoleta, debido a varias vulnerabilidades que pueden ser aprovechadas por los atacantes
Escritorio Remoto podrían permitir la ejecución de código remoto	122	CVE-2012-0002 CVE-2012-0152	Se refiere a una vulnerabilidad del protocolo RDP[8]
DNS[9] Cache snooping	14	N/A	Permite conocer que direcciones resuelve el servidor DNS, de esta manera se podría elaborar un ataque de secuestro de sesión o derivados, de acuerdo a los hábitos de navegación de los usuarios

[8] RDP: Protocolo de escritorio remoto, Remote Desktop Protocol por sus siglas en ingles.
[9] DNS: Servicio de nombre de dominio, Domain Name Service por sus siglas en ingles.

Escritorio remoto susceptible a ataques de hombre en el medio	168	CVE-2005-1794	Esta vulnerabilidad podría permitir que un atacante tome el control del equipo afectado, debido a un manejo inadecuado del manejo de sesiones
Múltiples Vulnerabilidades en HP Data Protector < 06.20	34	CVE-2011-0923 CVE-2011-728 CVE-2011-1729 CVE-2011-1730 CVE-2011-1731 CVE-2011-1732 CVE-2011-1733 CVE-2011-1734 CVE-2011-1735 CVE-2011-1736 CVE-2011-2399	Las vulnerabilidades detectadas podrían permitir ejecutar código remoto, elevación de privilegios tomando control total del equipo y su información.
Múltiples Vulnerabilidades en HP System Management	22	CVE-2008-1468 CVE-2008-4226 CVE-2008-5557 CVE-2008-5814 CVE-2009-1377 CVE-2009-1378 CVE-2009-1379 CVE-2009-1386 CVE-2009-1387 CVE-2009-4185 CVE-2010-1034	Las vulnerabilidades detalladas permiten evadir los controles de acceso permitiendo acceso a las consolas administrativas del servidor

		CVE-2010-1917 CVE-2010-2531 CVE-2010-2939 CVE-2010-2950 CVE-2010-3709 CVE-2010-4008 CVE-2010-4156 CVE-2011-1540 CVE-2011-1541	
HP Data Protector permite ejecución comandos	32	CVE-2011-0923	Esta vulnerabilidad permite en el caso de sistemas operativos Windows, la ejecución de comandos sin parámetros.
Sesiones nulas activas(Windows SMB NULL)	115	CVE-1999-0519 CVE-1999-0520 CVE-2002-1117	Permite utilizar credenciales nulas para autentificarse con el servidor, de esta manera se puede enumerar servicios y conocer algunas configuraciones del equipo.
Microsoft SQL Server ejecución de código remoto	13	CVE-2008-5416	Vulnerabilidad relacionada con la ejecución del código en el procedimiento almacenado extendido "sp_replwritetovarbin", en donde los parámetros no están bien filtrados.
Múltiple escalado de privilegios en Microsoft SQL	9	CVE-2008-0085 CVE-2008-0086 CVE-2008-0106	Vulnerabilidad que le permite a un usuario autentificado, escalar

Server		CVE-2008-0107	sus privilegios y tomar control de objetos y esquemas de la base de datos a los cuales no fue autorizado
Credenciales por defecto en Microsoft SQL Server	5	CVE-1999-0508	La cuenta “sa”, que forma parte de la instalación por defecto de Microsoft SQL Server, está configurada con la contraseña por defecto permitiendo que cualquier usuario ingrese con privilegios elevados a la base de datos.
Credenciales por defecto db2admin en Windows	36	CVE-2001-0051	La instalación de DB2 crea por defecto la cuenta db2admin, la cual puede ser usada para comprometer los servicios, bases de datos, credenciales de otros usuarios, e información almacenada.
Múltiples vulnerabilidades en Windows permiten la ejecución de código remoto	27	ms08-067 ms05-039 ms06-040 ms04-022 ms10-054 ms05-043 ms04-011	Permite ejecución de código remoto, debido a la falta de instalación de parches de seguridad, o a fallas en los servicios Plug and Play
Sistema operativo Obsoleto	3	N/A	La versión de Windows XP se considera obsoleta, debido a que su soporte oficial extendido finalizó el 8 de abril de 2014, y existen vulnerabilidades que ya no serán corregidas
Múltiples vulnerabilidades en Apache	5	CVE-2007-6750 CVE-2009-3555 CVE-2010-0408 CVE-2010-0425 CVE-2010-0434	Varias vulnerabilidades que permiten: evadir controles de acceso, denegación de servicio, ataques de

		CVE-2009-2699	hombre en el medio por falla en la renegociación de sesiones, elevación de privilegios, etc.
Múltiples vulnerabilidades en Apache Tomcat	2	CVE-2011-1184 CVE-2011-2204 CVE-2011-2526 CVE-2011-2729 CVE-2011-3190 CVE-2011-5062 CVE-2011-5063 CVE-2011-5064 CVE-2010-4172 CVE-2008-5515	Versiones de Tomcat, anteriores a la 2.2.34, son susceptibles a vulnerabilidades de ejecución de código remoto y cross site scripting y denegación de servicio
Credenciales por defecto en Tomcat	2	CVE-2009-3099 CVE-2009-3548 CVE-2010-0557 CVE-2010-4094	La contraseña de la consola administrativa está configurada con los valores por defecto, permitiendo el despliegue de cualquier aplicación que ejecute comandos a nivel de sistema operativo.
Múltiples Vulnerabilidades en PHP < 5.3.11	2	CVE-2011-4566 CVE-2011-4885 CVE-2012-0057 CVE-2012-0781 CVE-2012-0788 CVE-2012-0789 CVE-2012-0831 CVE-2012-1172	Varias vulnerabilidades que permiten ejecución de código remoto y denegación de servicio.
Credenciales por defecto en dispositivo Cisco	2	CVE-2001-0051	Las claves por defecto permiten el acceso total a la configuración del equipo, y por tanto puede poner en riesgo la infraestructura de comunicaciones
Múltiples Vulnerabilidades en Cisco IOS Software	17	CVE-2012-0385 CVE-2012-0382 CVE-2011-3271 CVE-2012-0384	Vulnerabilidades que permiten denegación de servicio por reinicio del equipo

		CVE-2011-0946	mediante la manipulación de paquetes.
DoS[10] por renegociación en protocolos TLS/SSL[11]	89	CVE-2011-1473	El protocolo TLS/SSL, requiere gran capacidad computacional para renegociar la sesiones de los usuarios, por tanto sino se controla la renegociación y el número de sesiones simultáneas, es fácilmente lograr una negación de servicio.
Acceso anónimo a FTP	14	N/A	Cualquier usuario puede conectarse al servidor ftp sin necesidad de proporcionar una contraseña, comprometiendo la información cargada en estos equipos.
Nombres por defecto en las comunidades SNMP[12]	43	CVE-1999-0186 CVE-1999-0254 CVE-1999-0472 CVE-1999-0516 CVE-1999-0517 CVE-1999-0792	Esta vulnerabilidad permite realizar cambios en las configuraciones de los sistemas utilizando los nombres de las comunidades por defecto.

Tabla 3.28. Objetivo de análisis para pruebas internas de Hacking Ético
Elaborado por el Autor

Resultados de la pruebas de Ingeniería Social

Las pruebas de ingeniería social se limitaron a recolectar información de forma pasiva de algunas instalaciones a las que se les permitió acceso a los consultores; es decir que no se utilizaron técnicas de manipulación directa sobre el personal de Seguros del Pichincha. La información que los consultores pudieron recolectar fue la siguiente:

[10] DoS: Denegación de servicio, Deny of service por sus siglas en inglés
[11] TSL/SSL: Transport Socket layer/Secure Socket, por sus siglas en inglés son protocolos que permiten encriptar comunicaciones a través de redes.
[12] SNMP: Protocolo simple de administración de redes, Simple Network Management Protocol por sus siglas en inglés

Información	Condición
Usuarios y contraseñas de equipos	Notas adhesivas colocadas sobre los propios equipos
Diagramas de red explícitos	Colocados en paredes y divisiones modulares de las oficinas
Documentos con información oficial de la empresa	Arrojados en los basureros sin ser destruidos de forma adecuada
Tablas de direccionamiento IP	Abandonados sobre escritorios o mesas de trabajo

Tabla 3.29. Información recolectada en pruebas de ingeniería social
Elaborado por el Autor

De la misma manera los consultores verificaron que los centros de datos permanecen abiertos y sin control a determinadas horas, en las cuales incluso se verificó que varios equipos son dejados encendidos sin bloquear sus respectivas sesiones.

Recomendaciones y planes de remediación para los resultados de las pruebas de Hacking Ético

Los resultados de las pruebas de Hacking ético, dieron como resultado una gran cantidad de vulnerabilidades en un número equivalente de equipos; con algunas excepciones en donde se determinó que un equipo puede estar afectado por más de una vulnerabilidad, y de la misma manera requiere un plan de remediación que contemple esta característica. Cada vulnerabilidad detectada fue valorada, utilizando criterios aceptados internacionalmente, de acuerdo a 3 parámetros: impacto, probabilidad de ocurrencia y riesgo, con el objetivo de priorizar los planes de remediación.

Las recomendaciones realizadas por la empresa consultora fueron clasificadas en 3 grupos principales: aplicación o software, infraestructura y gestión. Esta clasificación obedece al ámbito en donde el plan de remediación se enfocará, el alcance que este tendrá y los responsables o involucrados. Tomando en cuenta esta diferenciación, en la Tabla 3.30 se detalla las recomendaciones realizadas por la empresa consultora.

Ámbito	Recomendación	Responsables
Aplicación / Software	Instalar parches y actualizaciones de los sistemas operativos.	Coordinaciones de aplicaciones, datos y soporte usuarios
	Renovar software obsoleto.	
	Desactivar los servicios no utilizados	
	Instalar y actualizar software anti virus	
	Cambiar contraseñas y parámetros por defecto	
	Utilizar una política de contraseñas fuertes	
	Utilizar técnicas de programación segura	
	Eliminar o desactivar cuentas y usuarios por defecto	
	Utilizar del criterio de menor privilegio en la asignación de permisos	
	Depurar el contenido de los servidores web, publicar el contenido estrictamente necesario para servicios de intranet e internet.	
	Utilizar protocolos de comunicación segura donde sea posible	
	Personalizar las instalaciones de software, o no utilizar las instalaciones por defecto.	
	Activar opciones de seguridad opcionales	
Infraestructura	Instalar sistemas de prevención de intrusos	Coordinación de infraestructura y telecomunicaciones
	Actualizar el firmware de los dispositivos de red	
	Configurar equipos de seguridad perimetral utilizando el criterio de menor privilegio	
	Cambiar usuarios y contraseñas por defecto	
	Controlar el acceso a los puntos de red	
	Restringir el acceso físico a los centros de datos y equipos de red	
Gestión	Elaborar políticas y procedimientos de seguridad de la información	STIC, procesos, coordinaciones de aplicaciones, datos, soporte usuarios, e infraestructura y comunicaciones
	Definir políticas y estándares para el desarrollo y publicación de aplicaciones	
	Establecer pruebas periódicas de seguridad de aplicaciones e infraestructura	
	Establecer métodos de control y cumplimiento de las políticas y procedimientos de seguridad	
	Establecer políticas para el uso de contraseñas	
	Capacitar al personal y socializar las iniciativas de seguridad	

Tabla 3.30. Recomendaciones Hacking Ético
Elaborado por el Autor

Plan para definir las políticas y procedimientos faltantes relacionados con la seguridad de la información

El objetivo principal de este plan de mejora es establecer un marco de trabajo que permita administrar la seguridad de los activos de TI, en el que se definan las políticas, objetivos, procesos y procedimientos relacionados con la Seguridad de la Información con el fin de manejar el riesgo, mejorar la seguridad y entregar resultados alineados a

los objetivos de la organización. El plan propuesto de esta iniciativa se detalla en la Figura 3.7.

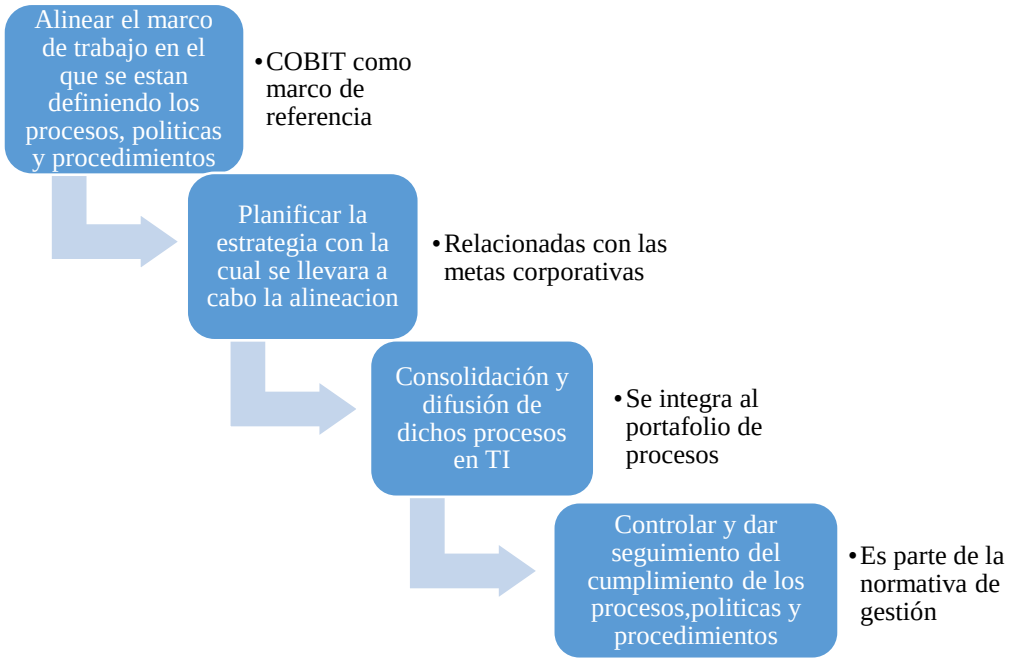


Figura 3.7. Plan para definir las políticas y procedimientos de Seguridad de la Información
Elaborado por el Autor

Plan para implementar Áreas de Seguridad de la Información

Los objetivos principales de esta iniciativa relacionados con el área de Seguridad de la Información son los siguientes:

- Definir los roles y funciones del personal del área de Seguridad de la Información
- Establecer su ubicación en la estructura organizacional fuera del área de TI

En la Figura 3.8 se define el plan de mejora para la creación del área de Seguridad de la Información de acuerdo a un esquema que resalta las principales fases de implementación, desde una definición en la cual participa el gobierno corporativo y la alta gerencia, hasta la definición de roles y actividades, de esta manera se pretende generar un área que responda a las necesidades empresariales de Seguridad de la Información y tenga el soporte y aceptación de todas las partes interesadas.(Mera Sebastian, 2014)

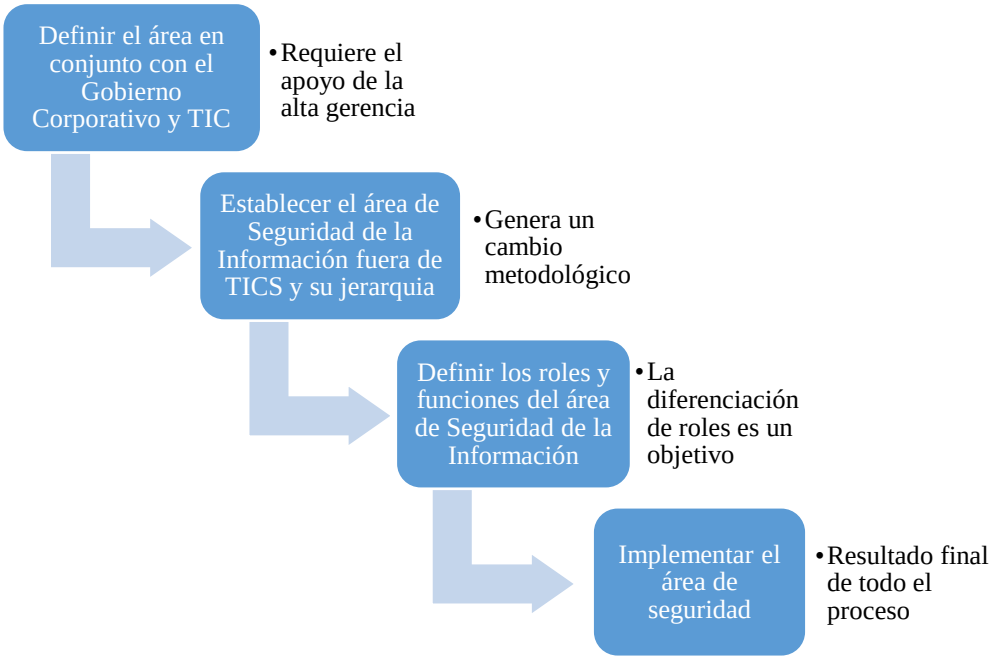


Figura 3.8. Plan para creación del área de Seguridad de la Información
Elaborado por el Autor

CONCLUSIONES

Al culminar el proyecto de la evaluación técnica e informática de los sistemas tecnológicos de información de Seguros del Pichincha, se han cumplido con los objetivos propuestos en el presente trabajo, por lo tanto se exponen a continuación las siguientes conclusiones

Para el desarrollo de una Auditoría Informática de los Sistemas de Información es de principal importancia contar con la guía de un marco de referencia. Para este proyecto se ha escogido el modelo COBIT desarrollado por ISACA, el cual a través de sus 5 dominios ofrece una serie de objetivos de gobierno que permiten evaluar eficientemente el ambiente de control de una entidad, garantizando que TI está alineada con el negocio y que los riesgos de TI se administren apropiadamente.

Al alinear la Normativa emitida por la Superintendencia de Bancos respecto a Tecnologías de la Información y los objetivos de control propuestos por COBIT se logró identificar y valorar los riesgos dentro de la entidad para tomar las medidas pertinentes y minimizar la materialización de los riesgos identificados.

Durante el análisis y evaluación del ambiente de control en la entidad aplicando los dominios propuestos por COBIT se logró identificar debilidades obteniendo observaciones y recomendaciones para ser emitidas en el informe final, para llevar a cabo el proceso de la Auditoría es de suma importancia contar con el compromiso y apertura a la Auditoría Informática de los sistemas de información; de los principales involucrados como son las Autoridades principales de Seguros del Pichincha, el personal del departamento de sistemas y el Departamento de Auditoría Interna.

RECOMENDACIONES

La Auditoría de TI en Seguros del Pichincha propone mejoras a los controles existentes en la misma, pues sabiendo que si los controles facilitan la rendición de cuentas mediante la evidencia; al mejorar los controles que están fallando se logrará mitigar los riesgos. La Administración debe identificarse y conocer plenamente los controles.

De acuerdo con lo planteado y el proyecto realizado es responsabilidad de la entidad aplicar y poner en marcha las recomendaciones emitidas de la Auditoría Informática, llevando a cabo esto de acuerdo a su capacidad y crecimiento.

Luego de la revisión se analizó el nivel de madurez en que actualmente se encuentra la empresa según los riesgos y fallas encontradas y se determina el nivel al que se puede ascender si se cumplen con las recomendaciones planteadas

BIBLIOGRAFIA

Barros Gabriela, Cadena Andrea (2012) Auditoria Informática de la cooperativa de ahorro crédito ‘‘Alianza del Valle’’Ltda. Aplicando Cobit 4.0. (Disertación de Ingeniería de Sistemas e Informática) Recuperada de repositorio.espe.edu.ec/xmlui/handle/21000/5197

Caridad Simón. S. (2006). Auditoría Informática. España. Obtenida el 18 de Noviembre del 2013, de http://www.scaridad.com/files/Apuntes%20de%20AI.pdf

Camacho, Antonio (2005) Herramienta para el análisis de requerimientos dentro de la pequeña empresa desarrolladora de software en Bogotá. (Disertación de Ingeniería de Sistemas). Recuperada de http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis189.pdf

COSO (Commite of Sponsoring Organization of the Theadway Commission, comite creado en 1985). Informe emitido en 1992 y modificado en 2204.

Duque, Natalia (2005) Comercialización de Seguros de vida a través del canal de mercadeo empresarial en Quito. Caso: Seguros del Pichincha. (Disertación de Licenciatura en Mercadotecnia). Recuperada de http://repositorio.ute.edu.ec/bitstream/123456789/10938/1/24966_1.pdf

Escuela Superior de Tlahuelipan. (2014). Auditoria Informática. Recuperado de http://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf

Hernández, E. Auditoria Informática: Un Enfoque Metodológico y Práctico. Continental. México. (1997).

Isaca (s.f.). COBIT 5. Madrid: Autor.

Isaca (s.f). COBIT 4. Madrid: Autor.

M@rtIn´s, (2014). ITIL, Information Technology Infrastructure Library. Recuperado de http://geeks.ms/blogs/mojeda/archive/2008/11/26/191-que-es-itil-information-technology-infrastructure-library.aspx

Mera, Sebastián (2014) Diseño del modelo de gestión de seguridad de la información del sistema erp de Ep Petroecuador de acuerdo a norma ISO/IEC 27002 y COBIT 5. (Disertación de Maestría en gerencia de redes y telecomunicaciones) Recuperada de http://repositorio.espe.edu.ec/handle/21000/8073

Piattini, M. G., Del Peso, E. Auditoria Informática: Un Enfoque Práctico. computec RAMA. España. (2003).

Quintuña, Veronica (2012) Auditoría Informática a la Superintendencia de Telecomunicaciones. (Disertación de Ingeniería de Sistemas) Recuperada de http://dspace.ucuenca.edu.ec/handle/123456789/652

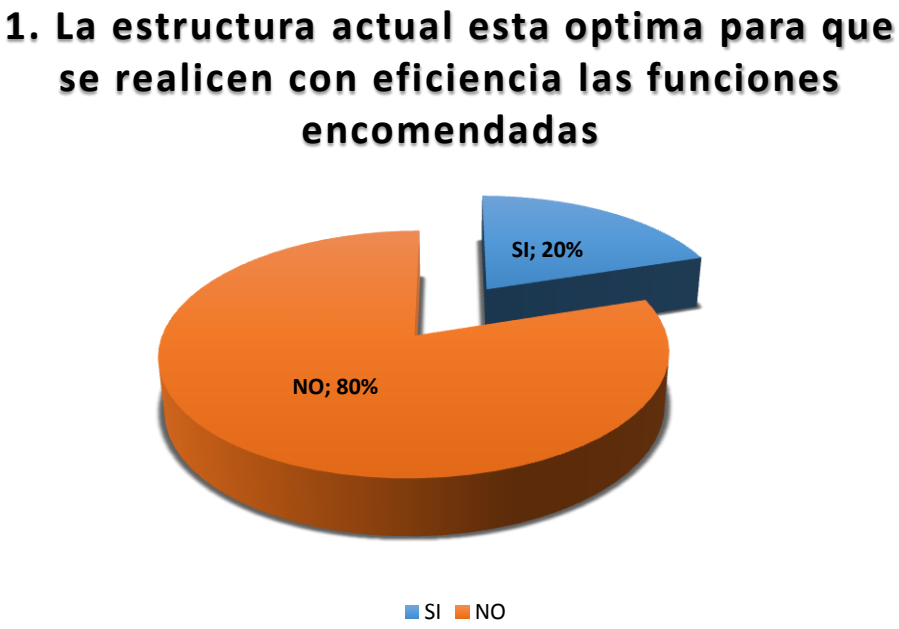
Seguros del Pichincha. (2014). Página web de Seguros del Pichincha. Recuperado de

http://www.segurosdelpichincha.com/

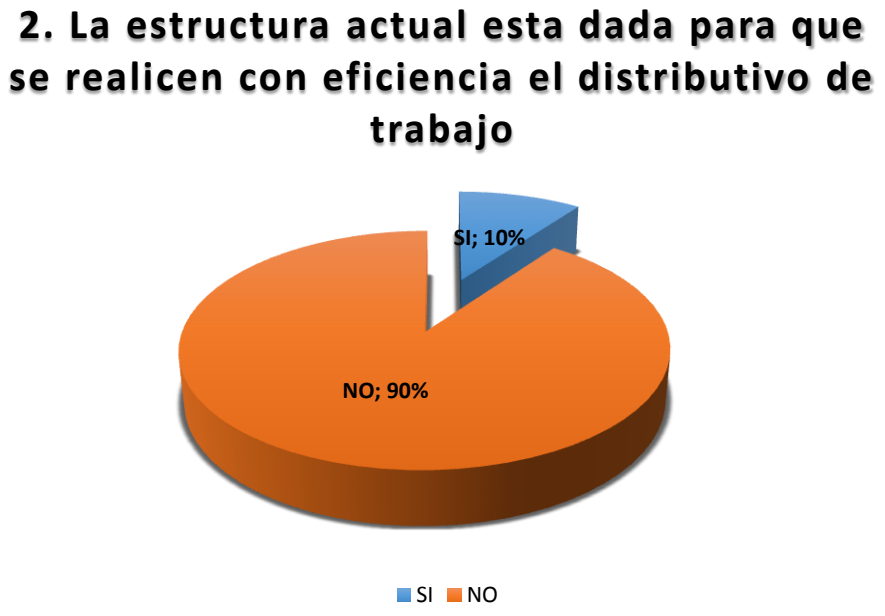
Yañez Carlos., Ibsen Sigfrid (2011) Trabajo de Investigación: Enfoque Metodológico de la Auditoría a las Tecnologías de Información y Comunicaciones. Recuperada de http://www.olacefs.com/Olacefs/ShowProperty/BEA%20Repository/Olacefs/uploaded/content/article/20120829_1.pdf

ANEXOS

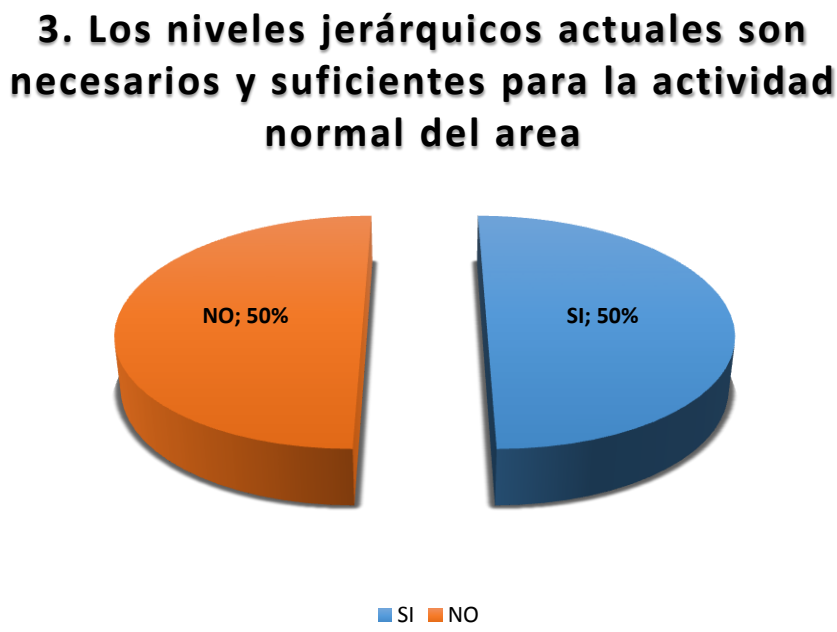
Anexo 1: Tabulación de encuestas A para la empresa Seguros del Pichincha s.a



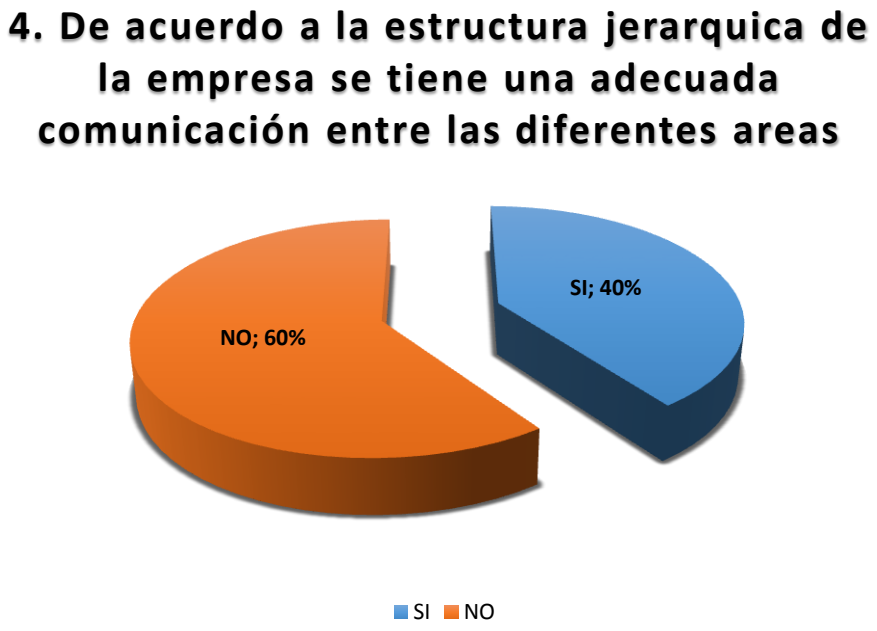
Al verificar la informacion obtenida la mayoria de empleados no esta de acuerdo con la estructura actual de la organización



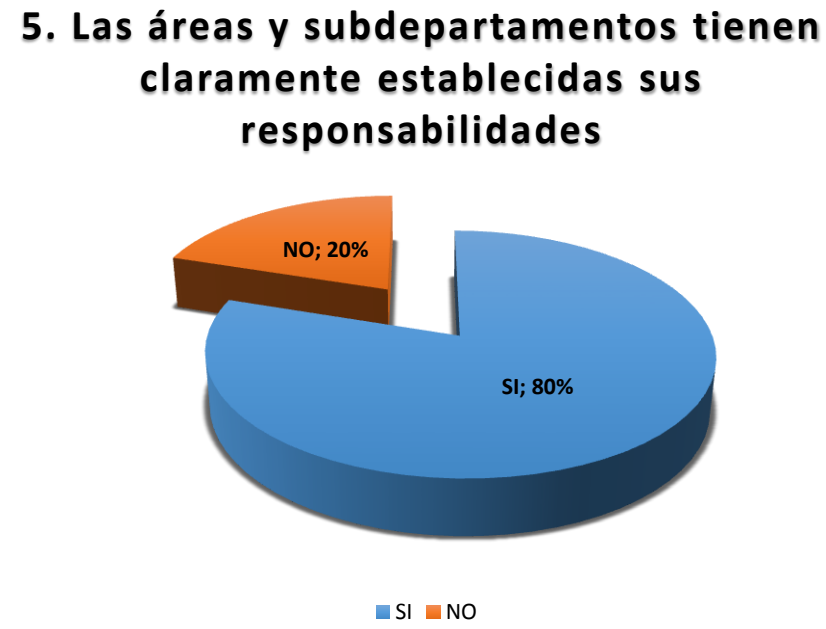
En Seguros del Pichincha la mayoría de empleados no está de acuerdo con la estructura actual por que no realizan con eficiencia su trabajo diario.



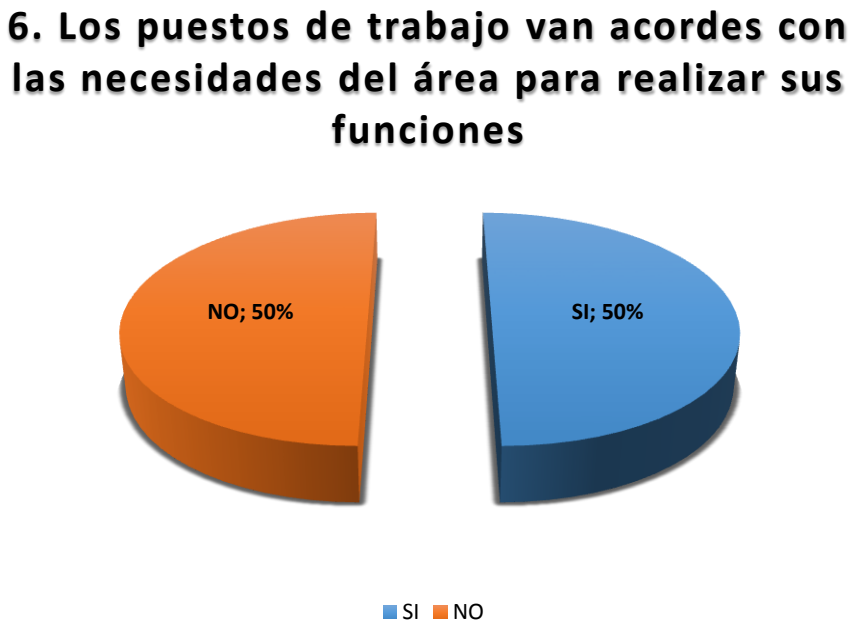
En la organización los niveles jerárquicos actuales tienen una aceptación parcializada en cada área consultada.



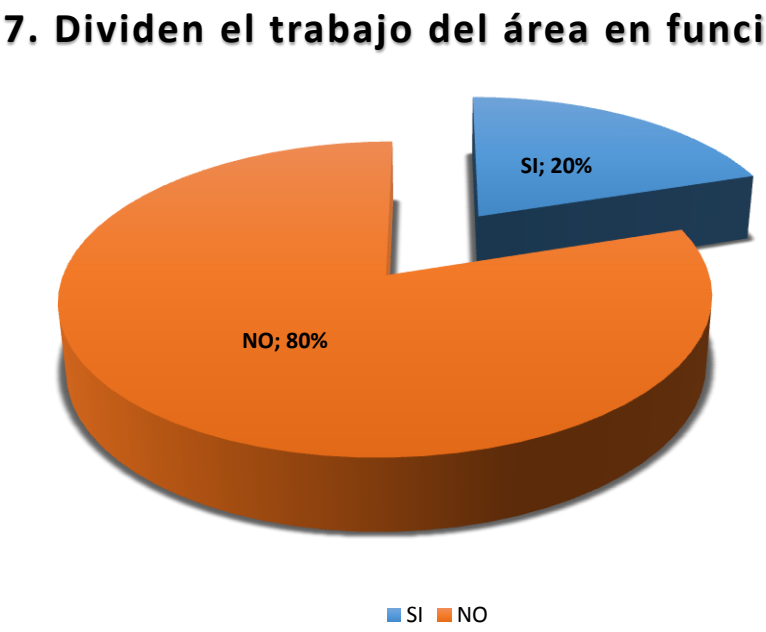
En la empresa no se tiene una correcta comunicación entre las diferentes áreas.



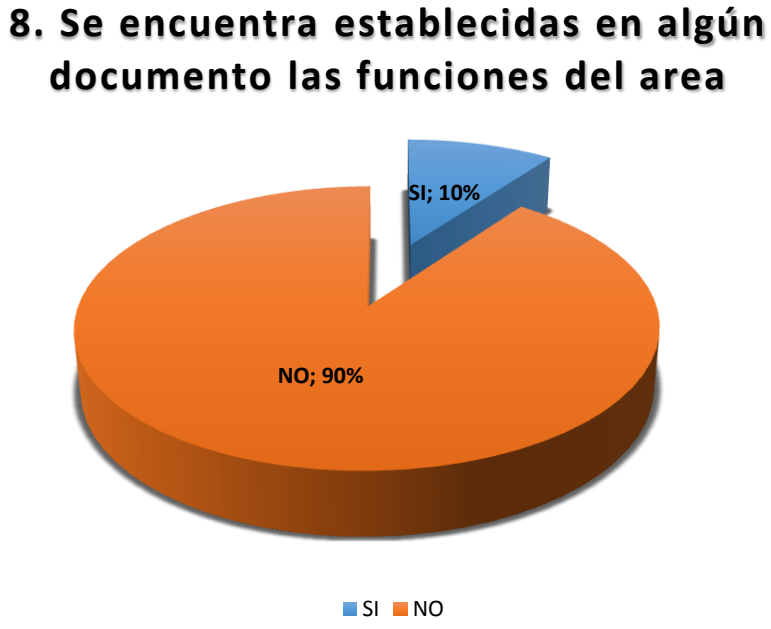
La mayoría de empleados tiene claro sus responsabilidades en su área establecida.



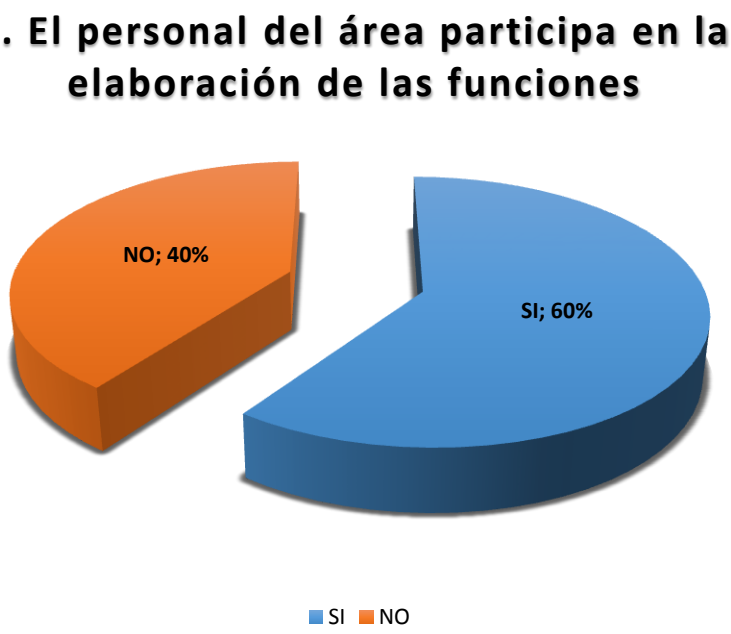
Al revisar se verifica que la mayoría de los empleados está dividida ya que ellos manifiestan que no existe un reparto funcional en la carga de trabajo en cada área.



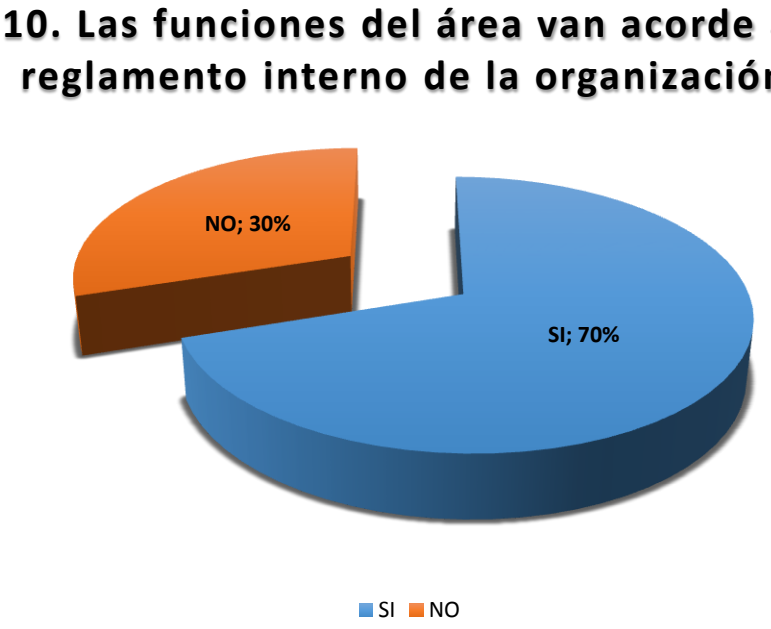
Se puede evidenciar que el trabajo no se divide en funciones en las áreas consultadas.



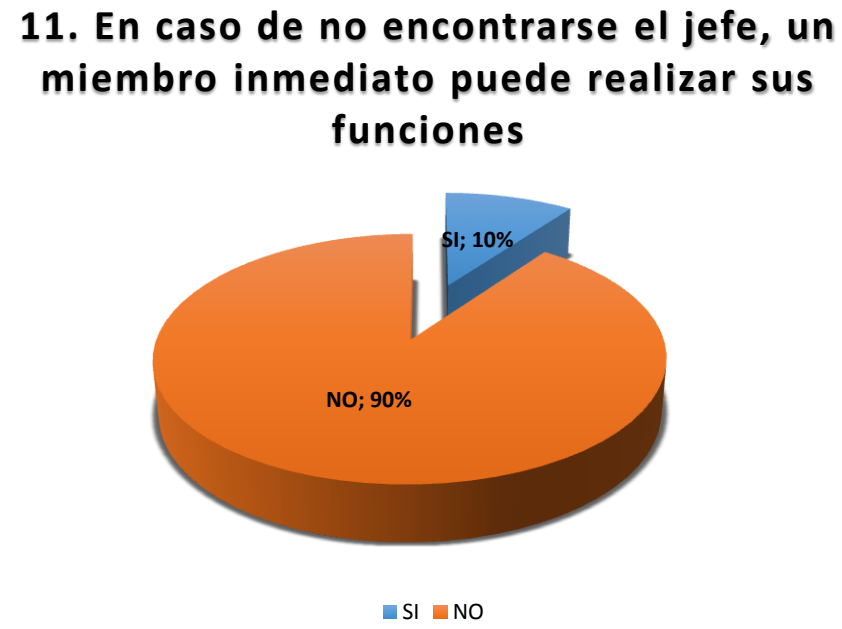
Los empleados verifican que las funciones del área no se encuentran impresas o registradas en algún documento.



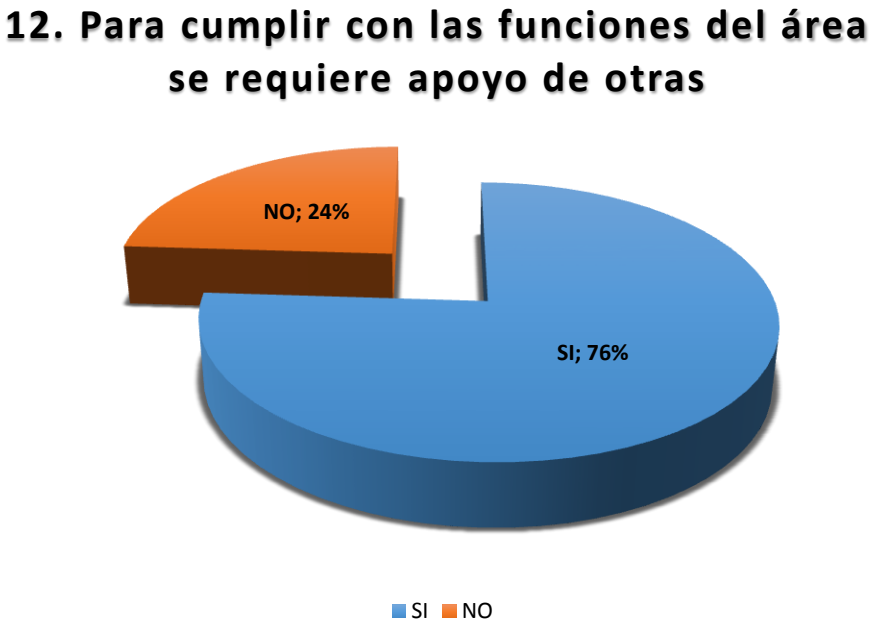
Como se manifiesta el personal tiene una participación elevada en la elaboración de las funciones.



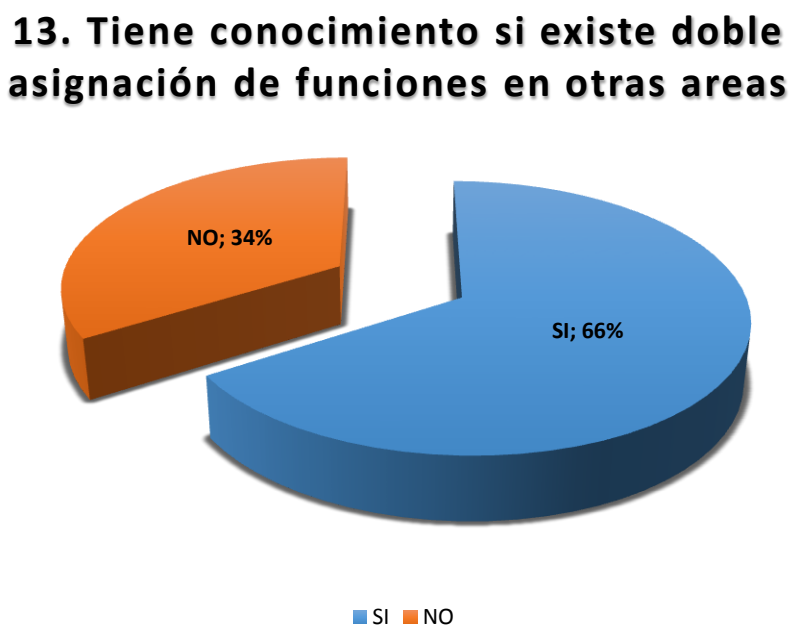
Se identifica que las funciones de cada área se encuentran en el reglamento interno pero no se cumplen las mismas.



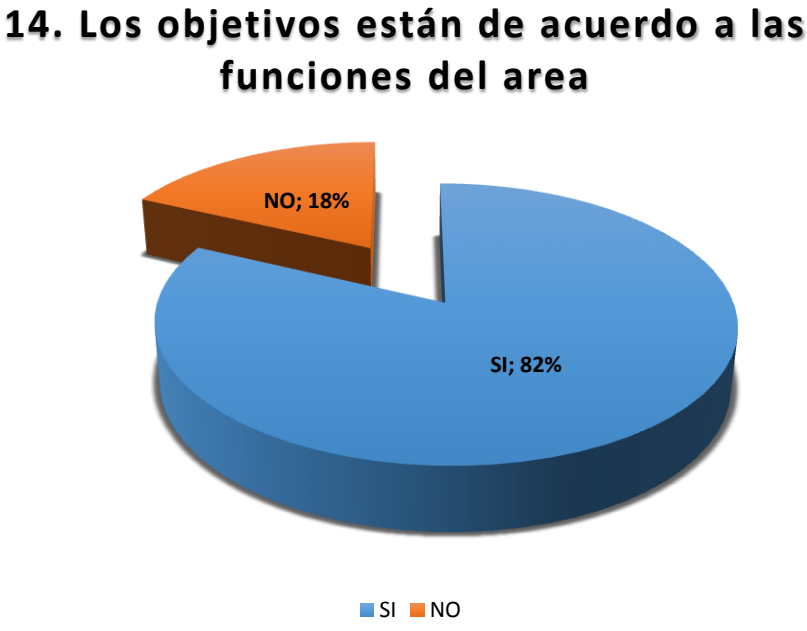
Como se dan cuenta en la organización ellos recomiendan que a falta del jefe inmediato no existe persona que realice sus funciones en la organización.



Se identifica que para el funcionamiento de cada área se necesita el apoyo de otras para un correcto funcionamiento de la organización

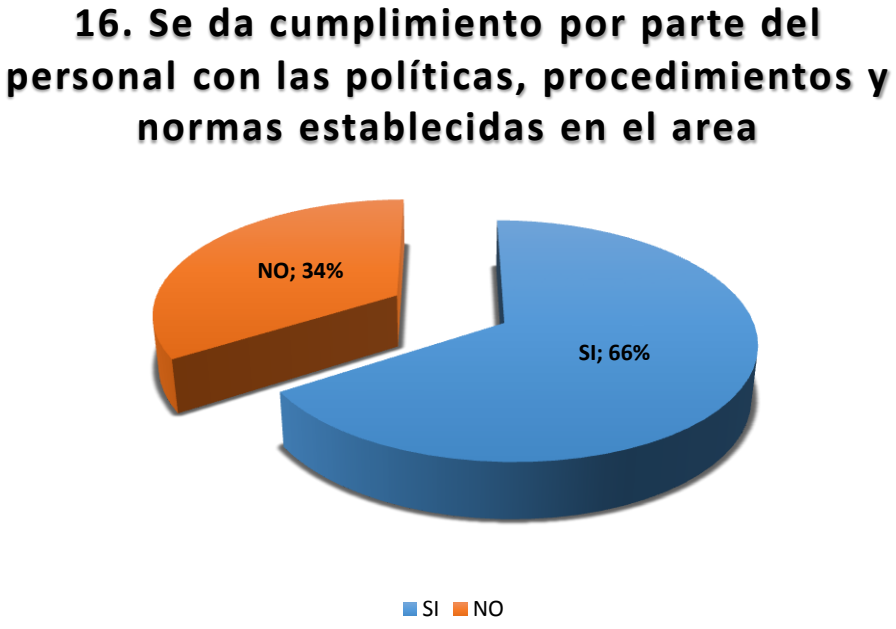


Se verifica que en algunas áreas existen empleados que realizan 2 funciones.



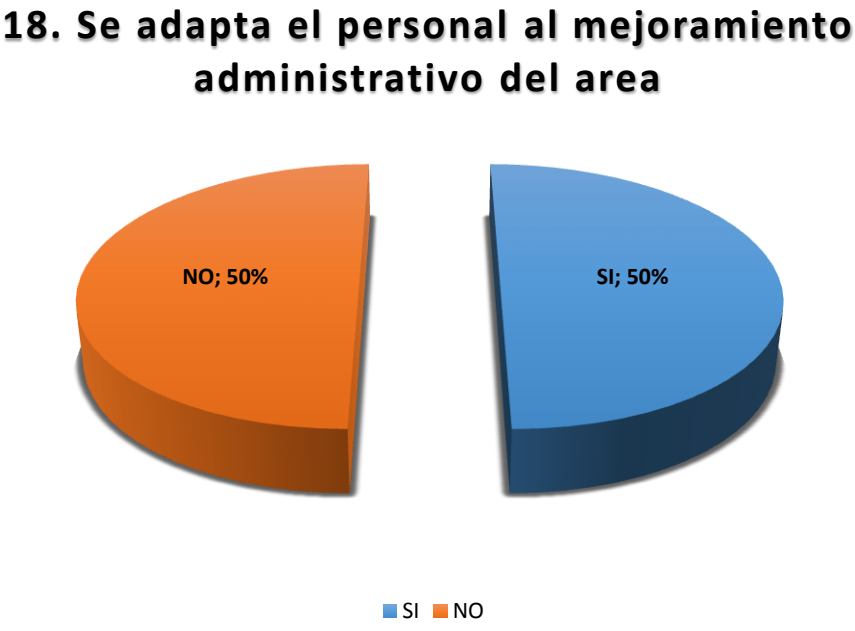
Se distingue que la mayoría está de acuerdo que las funciones del área están de acuerdo a sus objetivos estratégicos.

En la organización los empleados cuando existe falta de personal en determinada área realizan ellos la actividad para no afectar los procedimientos.

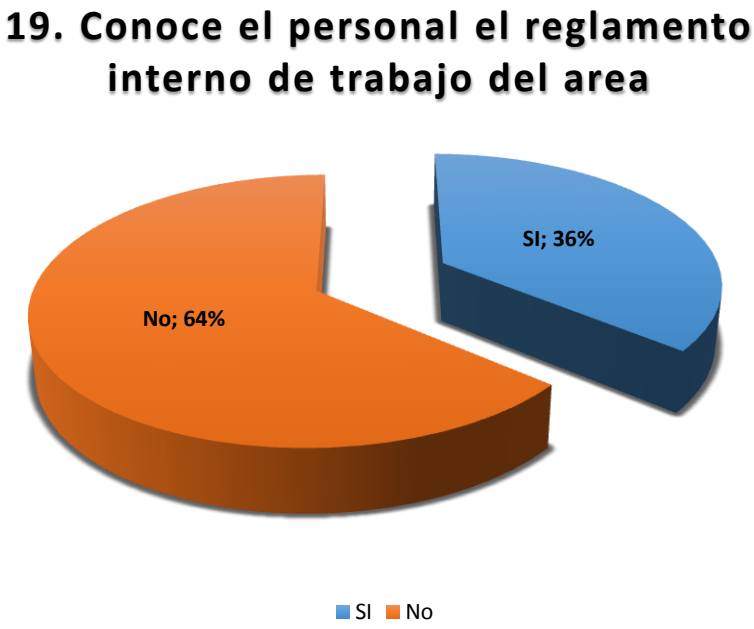


En la organización se cumple las políticas, procedimientos establecimientos en la empresa.

Se proporciona información que no existen políticas de seguridad claras cuando un empleado termina su relación laboral



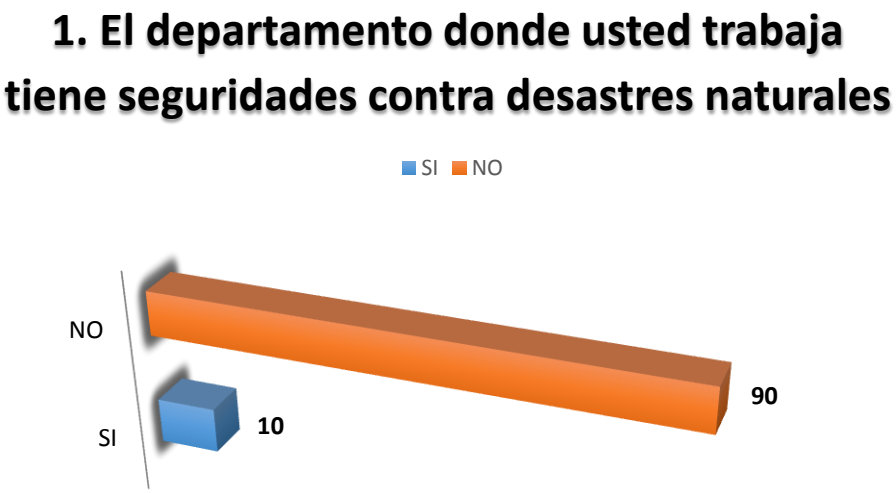
Se percata que el personal no se adapta fácilmente a los cambios administrativos establecidos en las diferentes áreas de la empresa.



La mayoría de empleados desconoce el reglamento interno de trabajo de cada área de la empresa.

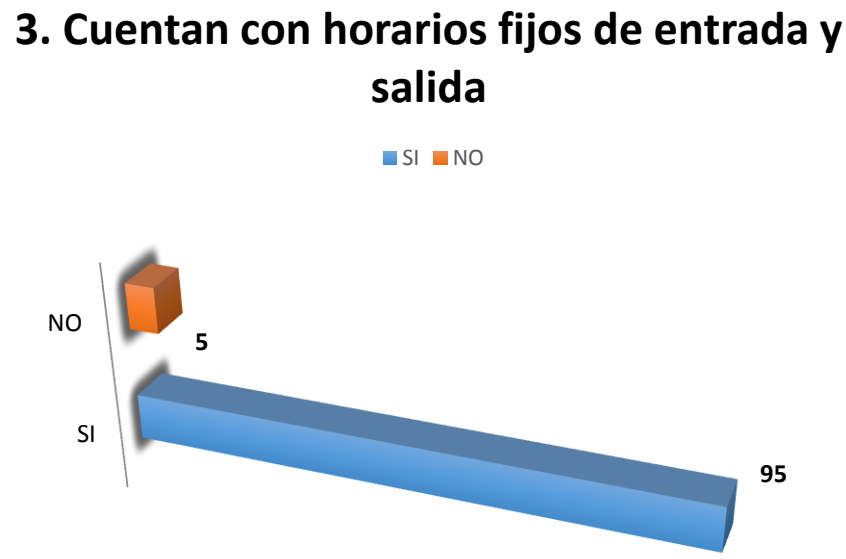
En cada área no tiene un plan de selección de personal si no existe un plan de selección de personal general de la compañía.

Anexo 2: Tabulación de encuesta B para la empresa Seguros del Pichincha s.a



Los empleados informan que en cada departamento no se tiene seguridades contra desastres naturales.

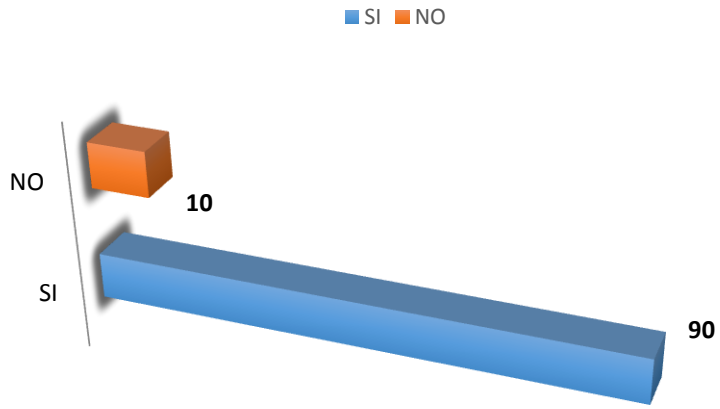
En la organización existe un plan de evacuación en cada departamento de Seguros del Pichincha.



En Seguros del Pichincha existen horarios establecidos de entrada y salida en cada departamento de la empresa.

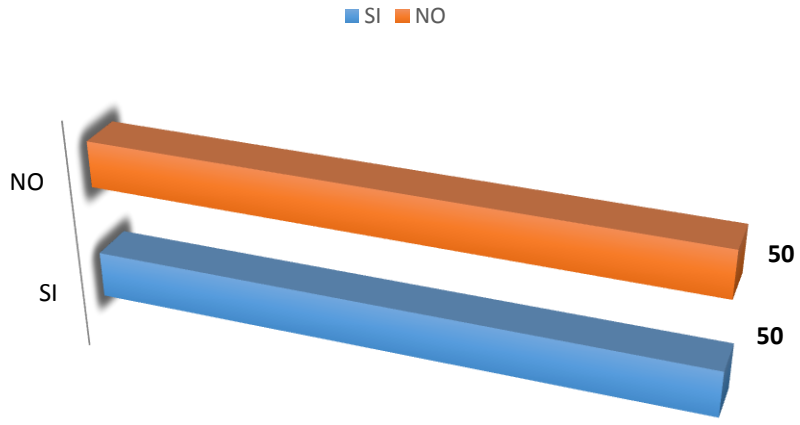
En la organización se lleva un control a medias del ingreso de personas a las diferentes áreas de Seguros del Pichincha

5. Existe alarmas para detectar el fuego, agua, calor o humo en forma automatica

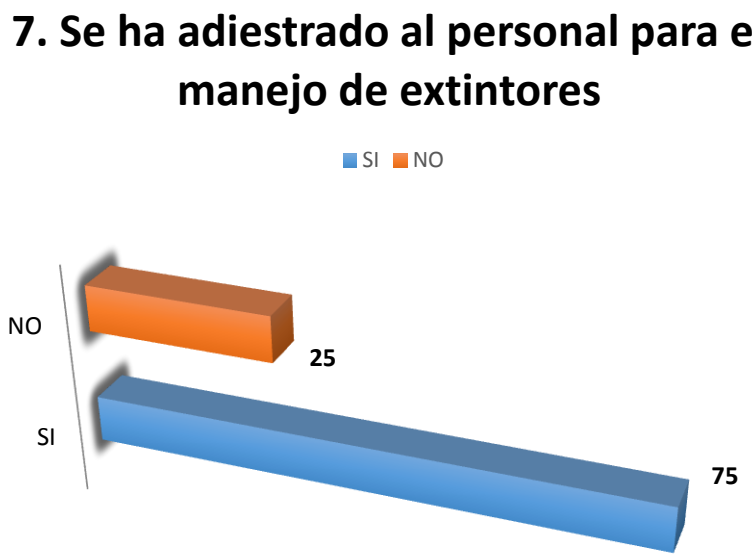


En la empresa los empleados indican que existen alarmas identificas por cualquier percance que existiera en la empresa.

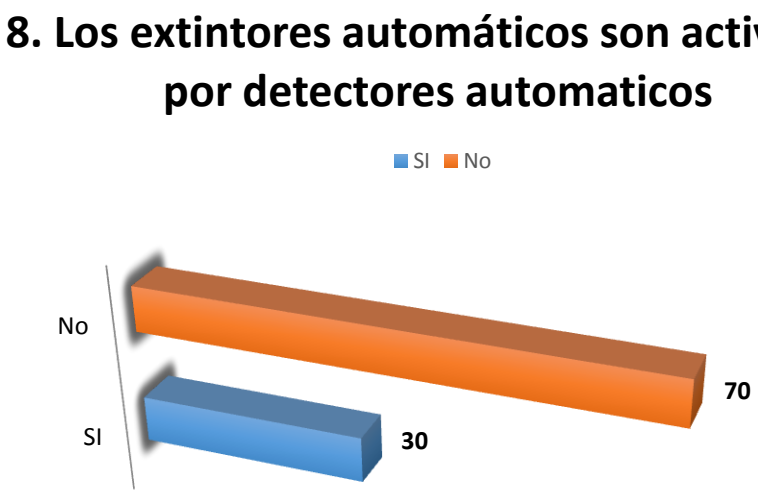
6. Existe en el departamento extintores de fuego



Se nos informa que en algunos departamentos, áreas existen extintores y en algunos otros no existe este recurso.

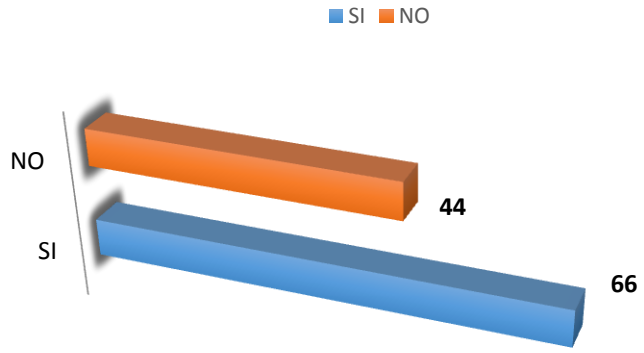


La mayoría de personas de la compañía tienen adiestramiento sobre el uso de extintores



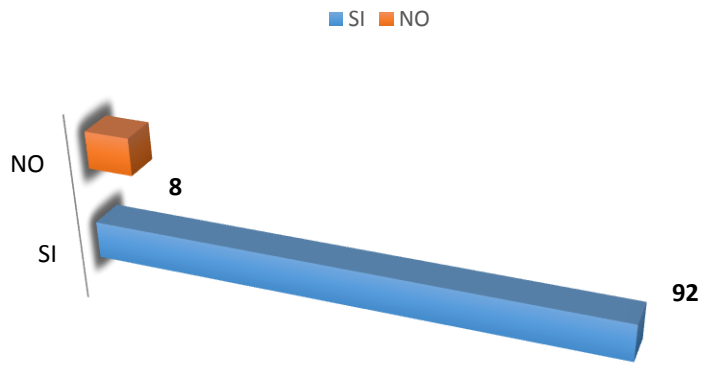
Los usuarios informan que no se posee detectores automáticos para la activación de los extintores automáticos en caso de Fuego

9. Los interruptores de energía eléctrica están debidamente protegidos, etiquetados, sin obstáculos para alcanzarlos



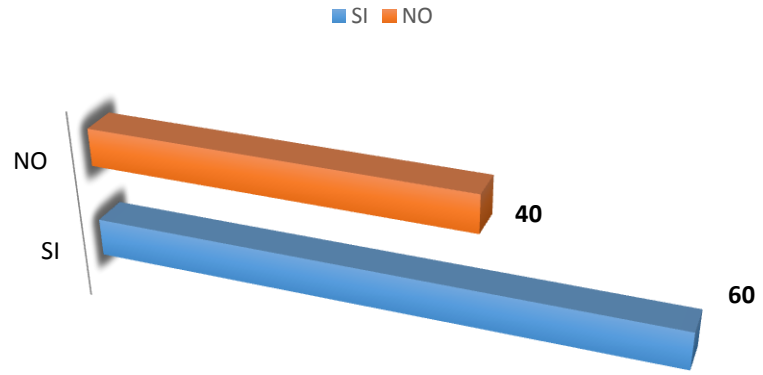
En la mayoría de la empresa se encuentra etiquetados los interruptores eléctricos en otras áreas no se cuenta con el etiquetado.

10. Saben que hacer los brigadistas de cada departamento en caso que ocurra una emergencia ocasionada por fuego



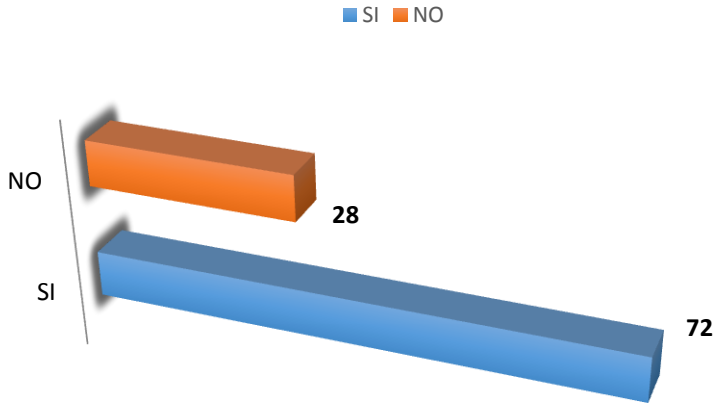
Los brigadistas están debidamente capacitados para cualquier siniestro que ocurra en Seguros Pichincha

11. Se ha adiestrado a todo el personal en la forma en que se debe desalojar las instalaciones en caso de emergencia



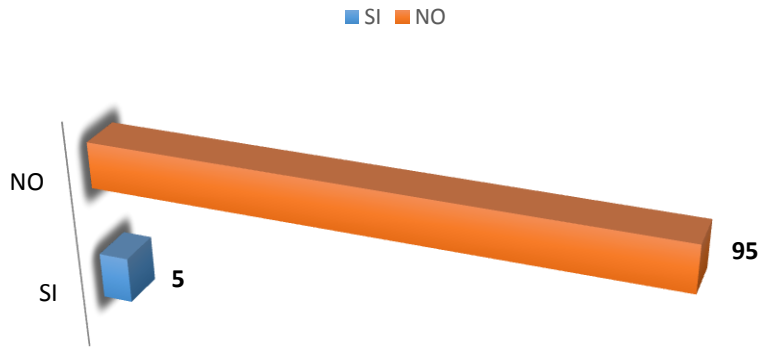
Se ha entrenado al personal como actuar en caso de emergencia en el establecimiento.

12. Se han tomado medidas para minimizar la posibilidad de fuego



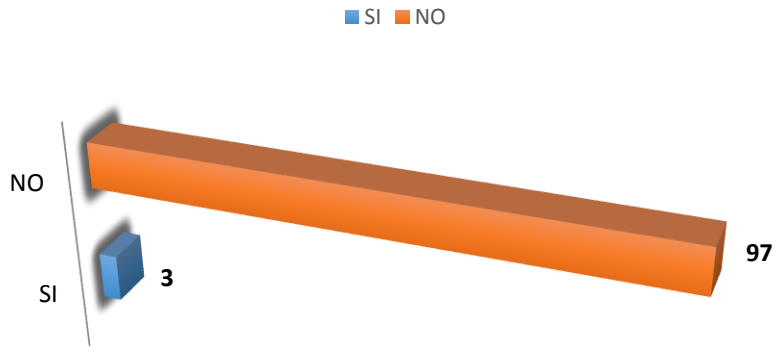
Se ha realizado medidas de seguridad para minimizar y mitigar la posibilidad de Fuego dentro de la compañía.

13. Se hace mantenimiento periódico a los computadores



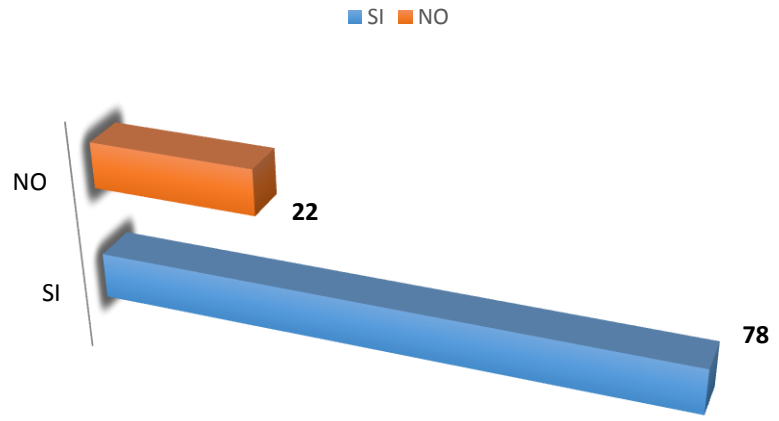
En los departamentos de la organización se informa que no se ha realizado un mantenimiento preventivo ni periódico de los equipos de computación.

14. Tiene conocimiento de la existencia de un plan de contigencia



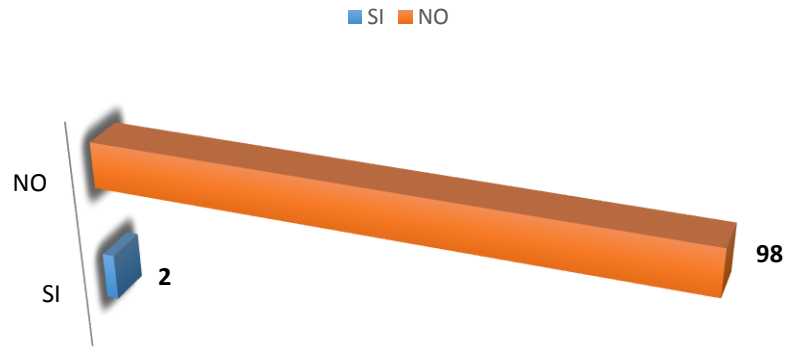
Se informa que no se tiene conocimiento sobre el plan de contingencia en la empresa.

15. Los cables de red, switch, hubs, etc. Se encuentran debidamente etiquetados



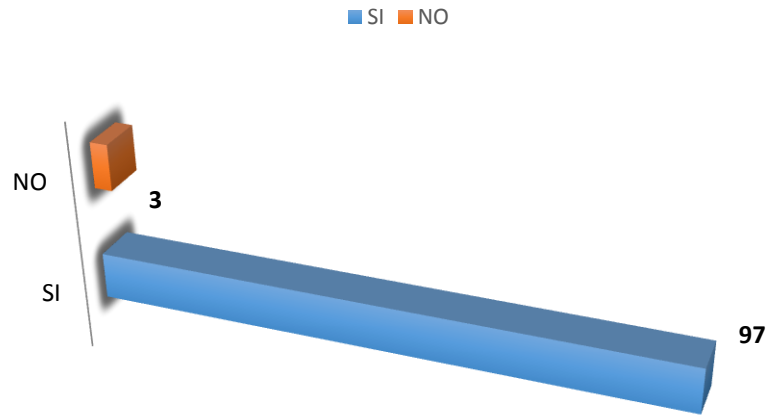
En la mayoría del establecimiento se encuentra debidamente etiquetados los puntos de red, switch. Etc.

16. El personal de limpieza esta preparado para manipular los dispositivos informaticos



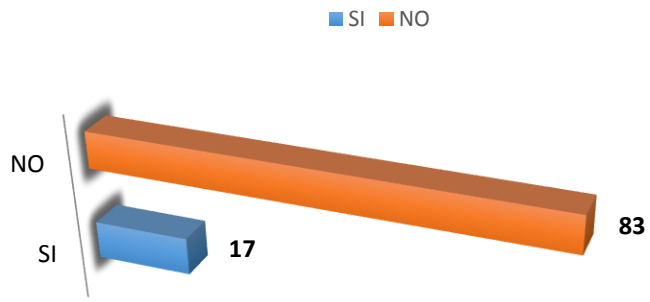
El personal de limpieza no está instruido ni capacitado en la manipulación de los dispositivos informáticos de la empresa.

17. Existen salidas de emergencia en caso de desastres



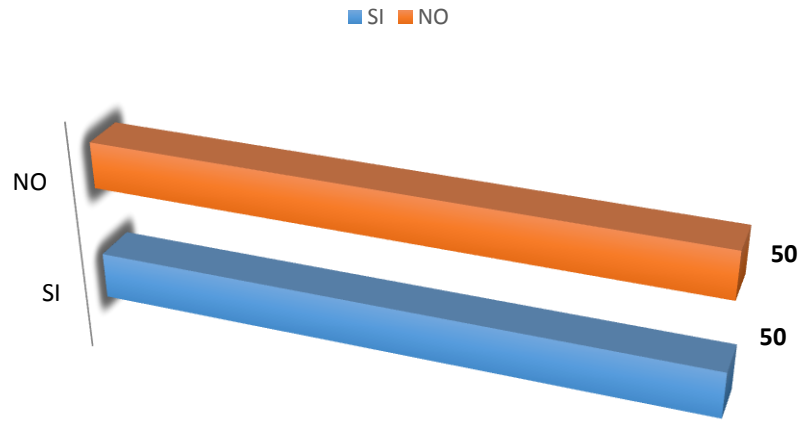
En la compañía existen salidas de emergencia debidamente señaladas e identificadas en cualquier percance existente.

18. Se vigila la moral y el comportamiento del personal con el fin de mantener una buena imagen



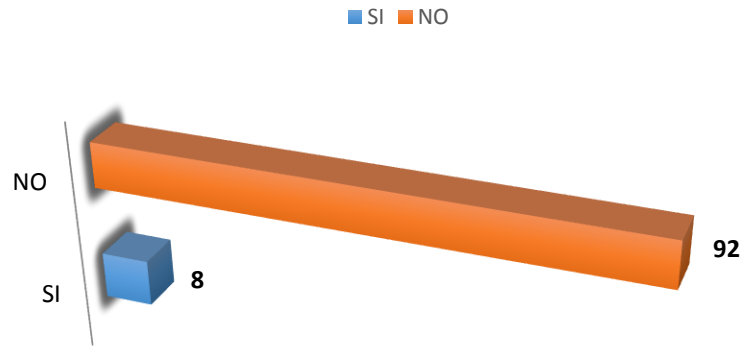
En los empleados no se controla la moral y el comportamiento del personal en Seguros del Pichincha s.a

19. Existe una persona responsable de la seguridad informática en su departamento



En la empresa no existe una persona fija que controle y verifique la seguridad informática en cada departamento perteneciente a Seguros del Pichincha s.a

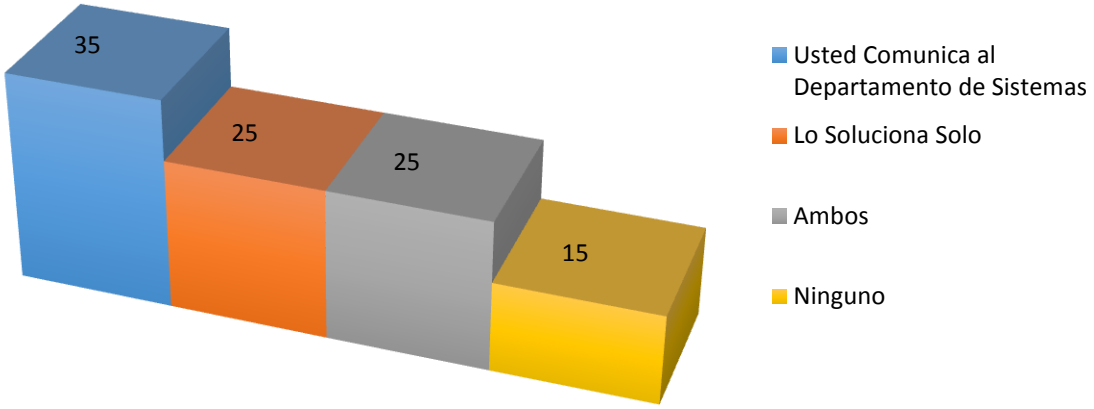
20. Existen alarmas para detectar otras condiciones anormales en el ambiente



En la organización no existen alarmas para detectar otro tipo de condiciones anormales en el ambiente.

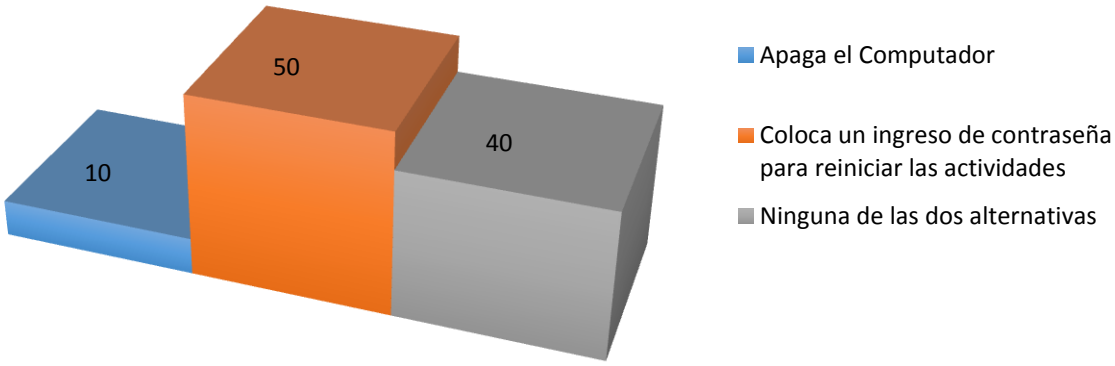
Anexo 3: Tabulación de encuesta C para la empresa Seguros del Pichincha s.a

1. Si tiene algún problema informatico



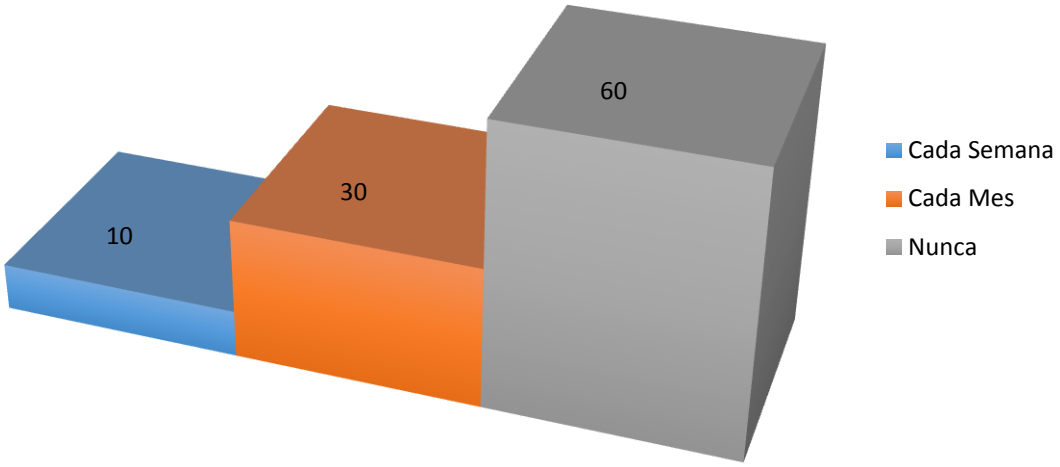
En la compañía la mayoría del personal trata de solucionar solo el problema y no comunica inmediatamente al Departamento de Sistema para su solución.

2. Cuando usted abandona su lugar de trabajo



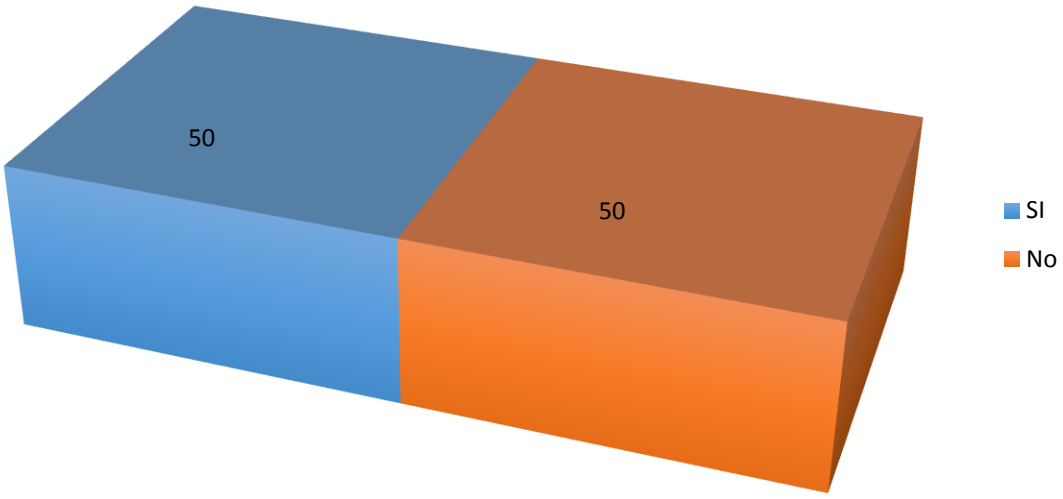
La mayoría de empleados no apaga su computador ni lo bloquea al equipo lo cual ocasiona un grave problema de seguridad informático.

3. Cada cuanto tiempo modifica la contraseña de su computador



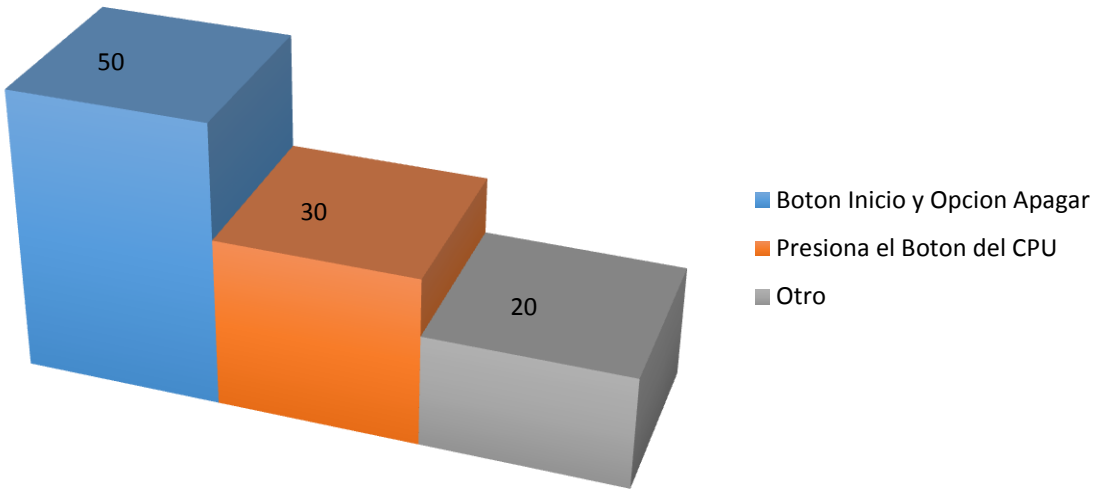
En la organización la mayoría del personal nunca cambia la contraseña de su computador.

4. Su computador tiene un UPS



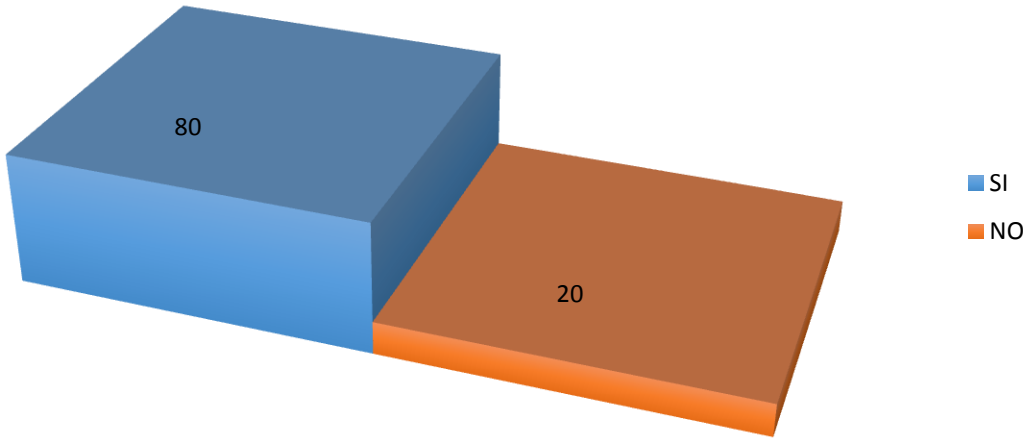
Es Seguros del Pichincha se informa que la mitad de los equipos no poseen o no están conectados al ups de la empresa.

5. Como apaga su computador



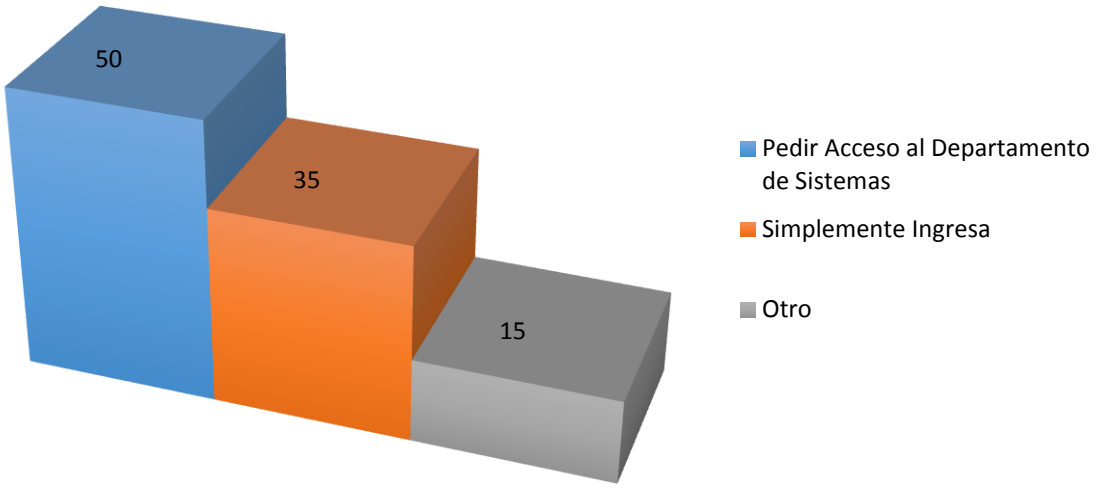
En SDP la mayoria apaga su computadora correctamente pero existe una parte que no apaga su computadora generando desperdicio de energia electrica.

6. Posee una contraseña personal para el uso del sistema de la empresa



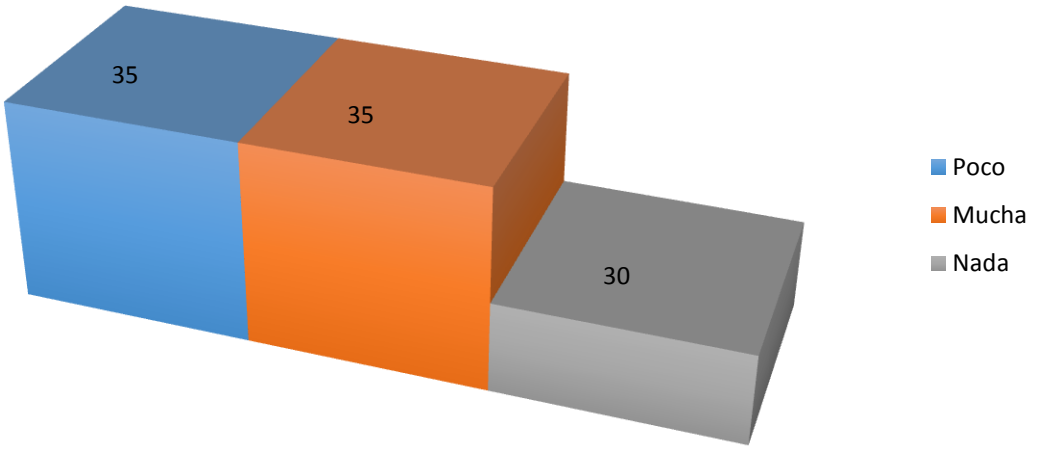
En SDP la mayoría de personal posee una contraseña personal en los sistemas informáticos de la empresa pero igual en otros sistemas no posees ninguna clave de acceso a los sistemas.

7. Para el uso del Internet usted necesita



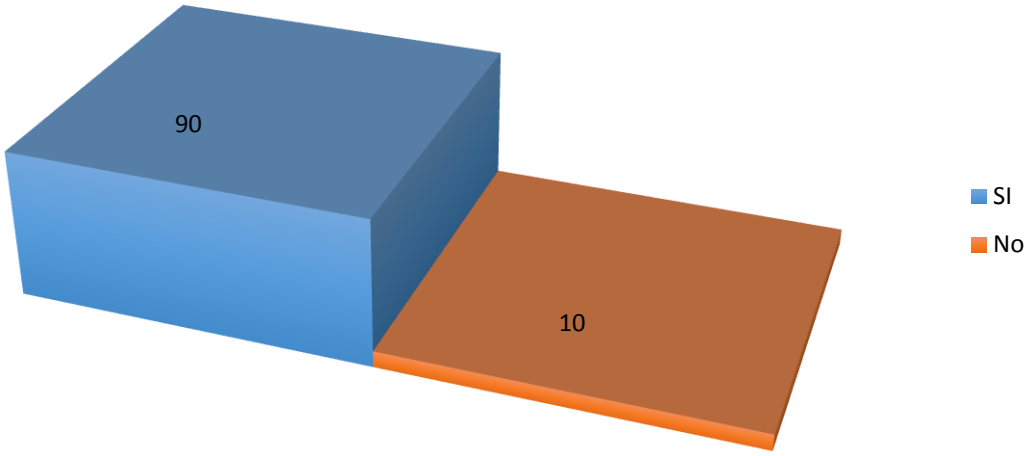
En la organización existe un alto procentaje que ingresan a internet sin ninguna restriccion a la red

8. Tiene conocimiento de todos los software instalados en su computador



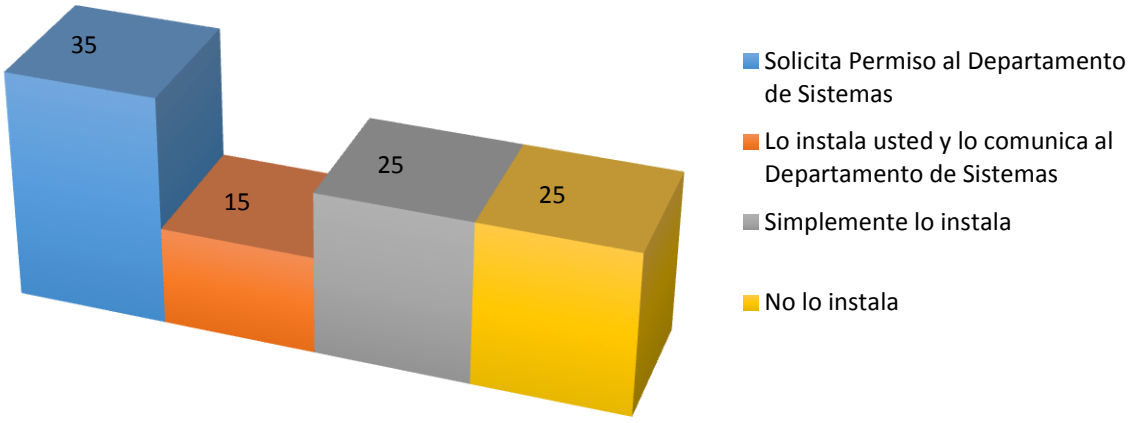
Los empleados no saben qué tipo de software tiene instalado en su computador

9. Cree que necesita una capacitación para el uso de sistemas nuevos en la empresa



Se proporciona información que la mayoría de empleados no sabe el uso correcto de los sistemas informáticos de Seguros del Pichincha s.a

10. Para instalar nuevo software en su computador



En SDP existe un alto porcentaje de software instalado en los equipos que no tienen nada que ver con el giro del negocio.

Anexo 4: Estándares de Software y Hardware

Sistemas Operativos:		
	Estaciones de Trabajo	Windows 8
		Windows 7
		Windows XP
	Servidores	Windows Server 64 bits
		AIX
		VMWARE
Software de Desarrollo:		
	Definido en las políticas de diseño de servicios(Proceso Diseño de Servicios)	
Software de Escritorio:		
	Oficina	Ms OfficeProfessional
	Graficadores	Corel Draw
		Visio
	Antivirus	McCaffe Corporativo
	Navegadores Internet	Internet Explorer
		Mozila Firefox
		Google Chrome
Otros		Ms Project
		WinRAR
		Adobe Acrobat Professional
Software de Soporte:		
	Administración de Red	
		Ip Route
		PRTG
		VNC
		WS_FTP
		Tivoli
		TeamViewer

Figura A4.1. Estándares de Software
Elaborado por el Autor

Servidor Tipo BLADE

Instalable en chasis H o S de IBM
Procesadores RISK o CISK
2 Procesadores instalados, desde 2,3 GHz y 4 core cada uno
2 Discos Duros ATA de 320 GB, 7200 rpm
Soporte para SAS RAID 1
Memoria Cache 1Mb L2 por Core
Memoria RAM 8 Gb DDR-2 exp. 64Gb
2 Puertos Fiber Channel
2 Puertos Gigabit Ethernet
Alimentación Electrica 120/240 VAC, 60Hz

Figura A4.2. Estándares de Hardware – Servidor tipo Blade
Elaborado por el Autor

Computadores de Escritorio

Tipo Desktop small form fractor
Procesador Core 2 Duo desde 2.33 Ghz, cache 4Mb L2
Disco SATA desde 250 Gb, 7200 rpm
Memoria RAM 4 Gb DDR2, exp 8 Gb desde 667 Mhz
Unidad de DVD-RW desde 52x16x52
2 Ranuras PCI para expansión
4 Puertos USB 2.0
1 Tarjeta de red 10/100/100 con puerto RJ-45
Fuente de poder desde 240 watt, con alimentación eléctrica 120VAC, 60hz
Monitor Lcd de 15” de la misma marca del CPU
Teclado PS/2 Latinoamericano de la misma marca que el CPU
Mouse PS/2 de 2 botones con scroll de la misma marca que el CPU
Licencia de Sistema Operativo Windows 8 Professional, 64 bits
Licencia de Sistema Operativo Windows 7 Professional, 64bits

Figura A4.3. Estándares de Hardware-Computadores de Escritorio
Elaborado por el Autor

Computadores Portátiles

- Procesador Core 2 Duo desde 1.8 Ghz, cache 2 MB L2
- Disco SATA desde 320 Gb, 5400 rpm
- Memoria RAM 4Gb DDR2, exp 8Gb desde 667 Mhz
- Unidad de DVD-RW desde 52x16x52
- 3 Puertos USB 2.0 incorporados
- 1 Puerto Gigabit Ethernet incorporada con conector RJ-45
- Wireless 802.11 a/b/g incorporado
- Conectividad Bluetooth
- Lector de Huella Digital
- Alimentación Eléctrica 120VAC, 60Hz
- Batería de Litio para 3 horas mínimo
- Monitor WXGA de 14”
- Teclado latinoamericano o español
- Mouse touchpad incorporado de 2 o 3 botones
- Licencia de Sistema Operativo Windows 7 Professional
- Licencia de Sistema Operativo Windows 8 Professional

Figura A4.4. Estándares de Hardware-Computadores Portátiles
Elaborado por el Autor

Impresoras:

- Multifunción Laser Monocromática
- Velocidad mínimo 70 ppm
- Resolución de Impresión 2400 Image Quality, 600x600 dpi
- Tamaño de Papel A4,A5,Eejcutivo, Legal, Carta, Sobre 10, Sobre B5
- Memoria Mínima 1024 Mb
- Disco Duro incluido 160 GB

Función de escáner a color en red
Función de Copia Monocromo
Velocidad mínima 70 cpm
Tarjeta de red 10/100/1000
Administración Web
Bandeja de Papel de 550 hojas

Láser Color
Velocidad mínima 25 ppm a Color
Velocidad mínima 25 ppm a B/N
Resolución de Impresión 1200 x 1200 dpi
Tamaño de Papel A4
Memoria Mínima 128 MB
Tarjeta de red 10/100/1000
Administración Web
Bandeja de Papel de 250 hojas

Figura A4.5. Estándares de Hardware – Impresoras
Elaborado por el Autor

Teléfonos:

- Tipo Business o Básico
- Soporte VozIp
- Función de Transferencia y captura de llamadas
- Manejo de correo de voz
- Switch 10/100 TX incorporado
- Alimentación Eléctrica PoE conforme al estándar IEEE 802.3af

Figura A4.6. Estándares de Hardware - Teléfonos
Elaborado por el Autor

Anexo 5: Planos y Matrices COBIT Desarrollados durante la ejecución de la Auditoria de Seguros del Pichincha

PLANO DE ENLACE DE LAS METAS DE LA INSTITUCION, METAS TI Y CRITERIOS DE INFORMACION																	
	METAS DE LA INSTITUCION		METAS DE TI								CRITERIOS DE INFORMACION DE COBIT						
											UTILIDAD	USABILIDAD	CREDIBILIDAD	LIBRE DE ERROR	ACCESIBILIDAD	CONFORMIDAD	SEGURIDAD
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI	24	28								X					
	2	Gestionar los riesgos de TI que afectan a la institución	2	14	17	18	19	20	21	22			X	X	X		
	3	Fomentar la Transparencia	2	18													X
Perspectiva del Cliente	4	Mejorar la orientación y servicio al usuario	3	23							X						
	5	Ofrecer productos y servicios competitivos	5	24							X	X					
	6	Establecer continuidad y disponibilidad de servicios	10	16	22	23					X				X		
	7	Crear agilidad en la respuesta a los cambios de los requerimientos institucionales	1	5	25						X	X					
	8	Lograr optimización de costos en la entrega de servicios	7	8	10	24						X					
	9	Obtener información fiable y útil para tomar decisiones estratégicas	2	4	12	20	26				X			X			X
Perspectiva Interna	10	Mejorar y mantener funcionalidad de los procesos institucionales	6	7	11						X	X					
	11	Reducir el costo de los procesos	7	8	13	15	24					X					
	12	Proporcionar cumplimiento con leyes, reglamentos y regulaciones	2	19	20	21	22	26	27				X			X	
	13	Proporcionar cumplimiento con políticas internas	2	13									X			X	
	14	Gestionar cambios institucionales	1	5	6	11	28				X	X					
	15	Mejorar y mantener operatividad en el control de las telecomunicaciones	7	8	11	13					X	X					
Perspectiva de Aprendizaje y Crecimiento	16	Gestionar productos e innovación en la institución	5	25	28						X	X					
	17	Adquirir y mantener personal cualificado y motivado	9								X	X					

Tabla A5.1. Plano de enlace de las metas de la institución, metas TI y Criterios de Información (COBIT 5, 2012)

PLANO DE ENLACE DE LAS METAS TI Y CRITERIOS DE INFORMACION											CRITERIOS DE INFORMACION DE COBIT						
	METAS DE LA INSTITUCION		PROCESOS DE TI-COBIT								UTILIDAD	USABILIDAD	CREDIBILIDAD	LIBRE DE ERROR	ACCESIBILIDAD	SEGURIDAD	CONFORMIDAD
Financiera	1	Alineamiento de TI y estrategia de negocio	EDM01	EDM02	APO01	APO02	APO03	APO05	BAI01	BAI02	P	P		S	S		
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	APO01	APO12	APO13	BAI10	DSS05	MEA02	MEA03		P	P					
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionas con TI	EDM01	EDM05							P	P		S	S		
	4	Riesgo del negocio relacionados con la TI gestionados	EDM03	APO10	APO12	APO13	BAI01	BAI06	DSS01	MEA01		S		P			S
	5	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	EDM02	APO04	APO05	APO06	APO11	BAI01			P	P		S			
	6	Transparencia de los costes, beneficios y riesgos de la TI	EDM02	EDM03	EDM05	APO06	APO12	APO13	BAI09		P	P				S	
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	BAI02	BAI03	BAI04	DSS01	DSS02	DSS04	DSS06	MEA01	P	P				S	
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	APO04	BAI05	BAI07						S	P					
Interna	9	Agilidad de las TI	EDM04	APO01	APO03	APO04	APO10	BAI08			P	P					
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones	EDM03	APO12	APO13	BAI06	DSS05				P	P	S	S	S	S	S
	11	Optimización de activos, recursos y capacidades de las TI	EDM04	APO01	APO07	BAI04	BAI10	DSS01	DSS03	MEA01	P	P		S	S		
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	APO08	BAI02	BAI07						P	P				S	S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	APO05	APO07	APO11	APO12	BAI01	BAI05			P	S					
	14	Disponibilidad de información útil y fiable para la toma de decisiones	APO09	APO13	BAI04	BAI10	DSS03	DSS04			S	S	P	P	P	S	S
	15	Cumplimiento de las políticas internas por parte de las TI	EDM03	APOO1	MEA01	MEA02					S	P					
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	EDM04	APO01	APO07						P	P		S	S		
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	EDM02	APO01	APO02	APO04	APO07	APO08	BAI05	BAI08	P	P	S	S	S	S	S

Tabla A5.2. Plano de enlace de las metas TI, Procesos COBIT y Criterios de información (COBIT 5,2012)

PLANO DE ENLACE DE LAS METAS TI Y CRITERIOS DE INFORMACION																					
			METAS RELACIONADAS CON LAS TI																		
			Alineamiento de TI y estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionas con TI	Riesgo del negocio relacionados con la TI gestionados	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de la TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de Negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y fiable para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
PROCESOS DE COBIT 5			FINANCIERA						CLIENTE		INTERNA							APRENDIZAJE Y CRECIMIENTO	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la entrega de beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la optimización del riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la optimización de los recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el marco de gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la arquitectura empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el presupuesto y los costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los recursos humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los acuerdos de servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	AP013	Gestionar la seguridad		P		P		P	S	S		P				P			

P= RELACION PRIMARIA S=RELACION SECUNDARIA

Tabla A5.3. Plano de enlace de las metas relacionados con las TI y los Procesos relacionados con TI (COBIT 5, 2012)

PLANO DE ENLACE DE LAS METAS TI Y CRITERIOS DE INFORMACION																			
			METAS RELACIONADAS CON LAS TI																
			Alineamiento de TI y estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionas con TI	Riesgo del negocio relacionados con la TI gestionados	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de la TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitacion y soporte de procesos de negocio integrando aplicaciones y tecnologia en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y fiable para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
PROCESOS DE COBIT 5			**FINANCIERA**						**CLIENTE**		**INTERNA**							**APRENDIZAJE Y CRECIMIENTO**	
Construcción, Adquisición e Implementación	BAI01	Gestionar los programas y proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la definición de requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la identificación y la construcción de soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la disponibilidad y la capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de cambios organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la aceptación del cambio y de la transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las peticiones y los incidentes del servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los servicios de seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los controles de los procesos del negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, evaluar y valorar rendimiento y conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, evaluar y valorar el sistema de control interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos		P		P	S		S			S					S		S

Tabla A5.4. Plano de enlace de las metas relacionados con las TI y los procesos relacionados con TI (COBIT 5, 2012)

Actividades específicas de seguridad para los procesos de COBIT 5

En esta sección se complementa la guía genérica "Procesos catalizadores COBIT 5", definiendo actividades de proceso con un enfoque en la Seguridad de la Información según ISO 27002, para los procesos cuya relación con las metas de TI sea principal 'P', de acuerdo a la Tabla A5.4. Adicionalmente, se selecciona las 2 metas principales, como un ejercicio práctico de priorización que sería de utilidad en cualquier otra implementación. Las metas seleccionadas, por ser las mayormente tratadas en esta investigación, son:

- Seguridad de la información, infraestructura de procesamiento y aplicaciones
- Alineamiento de TI y estrategia de negocio

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.

Actividades:

- Analizar e identificar factores legales, regulatorios y obligaciones contractuales que influencien en el diseño de gobierno de Seguridad de la Información.
- Definir principios que guíen el diseño de catalizadores para Seguridad de la Información y promocione un ambiente adecuado.
- Obtener comprometimiento de los niveles ejecutivos con la Seguridad de la Información y la gestión de riesgos.
- Alinear la estrategia de seguridad con la estrategia de negocio.

EDM02 Asegurar la entrega de beneficios

Actividades:

- Identificar y registrar los requerimientos de las partes interesadas para proteger sus intereses a través de la Seguridad de la Información.
- Establecer un método para demostrar el valor de la Seguridad de la Información, incluyendo una colección de información relevante.
- Dar seguimiento a las iniciativas de Seguridad de la Información y verificar la entrega de beneficios

EDM03 Asegurar la optimización de riesgos.

Actividades:

- Controlar el nivel de integración de la gestión de riesgos de la información con la gestión de riesgos corporativa.
- Definir niveles de riesgo aceptados, para mantener un equilibrio entre los riesgos y las oportunidades de negocio.

APO01 Gestionar el marco de gestión de TI

Actividades:

- Definir las funciones de seguridad, incluyendo roles internos y externos (Jefe de seguridad, Analista de seguridad).
- Determinar los grados de responsabilidad con la Seguridad de la Información de los roles externos y comunicarlos.
- Alinear la organización de la seguridad de la información con los modelos organizacionales empresariales.
- Planificar evaluaciones continúas para determinar cumplimiento con políticas y procedimientos de Seguridad de la Información.

APO03 Gestionar la estrategia

Actividades:

- Entender como la S-I soportaría las metas empresariales tomando en cuenta las necesidades de las partes interesadas.
- Desarrollar criterios claros relacionados con la Seguridad de la Información y priorizar la atención de no cumplimientos o brechas.

APO07 Gestionar los recursos Humanos

Actividades:

- Asegurarse que los requerimientos de seguridad se apliquen en los procesos de reclutamiento de empleados y contratistas.
- Proporcionar desarrollo profesional con programas de capacitación en

Seguridad de la Información.

- Establecer criterios de Seguridad de la Información en la evaluación de personal

APO08 Gestionar las Relaciones

Actividades:

- Entender el negocio y como la Seguridad de la Información afecta o facilita las actividades de este.
- Establecer un enfoque para influir contactos claves con respecto a la Sistemas de Información
- Incorporar requerimientos de Seguridad de la Información en los procesos de mejora continúa.

APO12 Gestionar El riesgo

Actividades:

- Identificar y recolectar información que habilite la identificación de riesgos relacionados con Seguridad de la Información.
- Identificar, analizar y evaluar el riesgo de la información.
- Monitorear continuamente los riesgos de la información
- Aplicar procesos de mitigación de riesgos específicos.

APO13 Gestionar la seguridad

Actividades:

- Definir el ámbito y alcance del SGSI, en términos de negocio, organización, localización, activos y tecnología.
- Definir el SGSI en concordancia con las políticas, normativa y marco legal vigente en la empresa.
- Verificar periódicamente la efectividad del SGSI, incluyendo política, objetivos, prácticas, etc.
- Llevar a cabo auditorías internas al SGSI.
- Registrar acciones y eventos que pueden tener un impacto en la efectividad y desempeño del SGSI.

BAI01 Gestionar programas y proyectos

Actividades:

- Incorporar Seguridad de la Información en los requerimientos y los estudios de factibilidad para cada proyecto que forme parte de los programas.

- Establecer un proceso para asegurar que toda la información relacionada al proyecto, recolectada o generada, sea segura.
- Desarrollar un plan de Seguridad de la Información que identifique el ambiente y controles a ser implementados para proteger los activos organizacionales.
- Integrar Seguridad de la Información en la gestión de proyectos de TI y de negocio.
- Realizar evaluaciones periódicas para asegurar que los requerimientos de Seguridad de la Información están siendo implementados.

BAI02 Gestionar definiciones de requerimientos

Actividades:

- Investigar, definir y documentar requerimientos de Seguridad de la Información, relacionados con confidencialidad, integridad y disponibilidad.
- Analizar los requerimientos de Seguridad de la Información con las partes interesadas y los implementadores técnicos.
- Llevar a cabo una valoración de riesgos para identificar los controles de Seguridad de la Información relevantes para las actividades empresariales.
- Validar los requerimientos de Seguridad de la Información con las partes interesadas y los implementadores técnicos.

BAI06 Gestionar cambios

Actividades:

- Asegurar que se lleve a cabo una evaluación de los potenciales impactos en la Seguridad de la Información provocados por los cambios.
- Asegurar que la política de Seguridad de la Información se adapta a las necesidades del negocio.
- Desarrollar prácticas para considerar el impacto en la Seguridad de la Información de las amenazas y tecnologías emergentes.

DSS05 Gestionar servicios de seguridad

Actividades:

- Sensibilizar sobre el software malicioso y hacer cumplir los procedimientos de prevención y responsabilidades.

- Instalar herramientas para protección contra software malicioso con opciones de actualización de definiciones activadas.
- Distribuir todo el software de protección centralizado, con opciones de configuración y actualización centralizada.
- Filtrar el tráfico entrante, para protegerse contra información no solicitada.
- Realizar actividades de entrenamiento relacionado con malware y métodos para navegación segura en internet.
- Establecer y mantener una política de seguridad para la conectividad en relación a la valoración de riesgos de la empresa.
- Cifrar la información en tránsito de acuerdo a su clasificación.
- Establecer mecanismos confiables para soportar la transmisión y recepción de información.
- Llevar a cabo pruebas periódicas de la seguridad de los sistemas para determinar idoneidad de las configuraciones realizadas.
- Configurar los sistemas operativos de forma segura.
- Implementar mecanismos de bloqueo automático.
- Cifrar la información en discos y respaldos de acuerdo a la clasificación de la información.
- Gestionar las conexiones remotas y accesos (VPN, oficinas remotas).
- Proteger la integridad de los equipos
- Disponer o desechar equipos terminales de forma segura.
- Mantener accesos a los sistemas de acuerdo a los roles y responsabilidades asignadas.
- Realizar revisiones periódicas de las cuentas y privilegios asignados.
- Asegurarse que todos los usuarios y sus actividades, sean identificadas de forma única.
- Registrar toda la información relacionada con incidentes de Seguridad de la Información, que permitan realizar análisis de causa-efecto.

PLANO DE ENLACE DE LAS METAS CORPORATIVAS DE COBIT 5 Y LAS METAS RELACIONADAS DE TI																			
			METAS RELACIONADAS CON LAS TI																
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgo de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia Financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas agiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
Meta relacionada con las TI			**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
PROCESOS DE COBIT 5			**FINANCIERA**					**CLIENTE**					**INTERNA**					**APRENDIZAJE Y CRECIMIENTO**	
FINANCIERA	1	Alineamiento de TI y estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgo del negocio relacionados con la TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de la TI	S		S		P				S	P		P					
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
INTERNA	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y fiable para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
APRENDIZAJE Y CRECIMIENTO	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Tabla A5.5. Plano de enlace de las metas corporativas de COBIT 5 y las metas relacionadas con TI (COBIT 5, 2012)

PLANO DE RESPONSABILIDADES DE COBIT					
PROCESOS DE TI – COBIT		**RESPONSABLE**			
		Departamento de TI	Dentro de la Institución	Externo	No se sabe con certeza
Evaluar, Orientar y Supervisar					
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno	X			
EDM02	Asegurar la entrega de beneficios	X			
EDM03	Asegurar la optimización del riesgo	X			
EDM04	Asegurar la optimización de los recursos	X			
EDM05	Asegurar la transparencia hacia las partes interesadas	X			
Alinear, Planificar y Organizar					
APO01	Gestionar el marco de gestión de TI	X			
APO02	Gestionar la estrategia	X			
APO03	Gestionar la arquitectura empresarial	X			
APO04	Gestionar la innovación	X			
APO05	Gestionar portafolio	X			
APO06	Gestionar el presupuesto y los costes	X			
APO07	Gestionar los recursos humanos	X			
APO08	Gestionar las relaciones	X			
APO09	Gestionar los acuerdos de servicio	X			
APO10	Gestionar los proveedores	X			
APO11	Gestionar la calidad	X			
APO12	Gestionar el riesgo	X			
AP013	Gestionar la seguridad	X			
Construcción, Adquisición e Implementación					
BAI01	Gestionar los programas y proyectos	X			
BAI02	Gestionar la definición de requisitos	X			
BAI03	Gestionar la identificación y la construcción de soluciones	X			
BAI04	Gestionar la disponibilidad y la capacidad	X			
BAI05	Gestionar la introducción de cambios organizativos	X			
BAI06	Gestionar los cambios	X			
BAI07	Gestionar la aceptación del cambio y de la transición	X			
BAI08	Gestionar el conocimiento	X			
BAI09	Gestionar los activos	X			
BAI10	Gestionar la configuración	X			
Entregar, dar Servicio y Soporte					
DSS01	Gestionar las operaciones	X			
DSS02	Gestionar las peticiones y los incidentes del servicio	X			
DSS03	Gestionar los problemas	X			
DSS04	Gestionar la continuidad	X			
DSS05	Gestionar los servicios de seguridad	X			
DSS06	Gestionar los controles de los procesos del negocio	X			
Supervisión, Evaluación y Verificación					
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad	X			
MEA02	Supervisar, evaluar y valorar el sistema de control interno	X			
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos	X			

Tabla A5.6. Plano de responsabilidades de Procesos COBIT (COBIT 5, 2012)

MATRIZ DE GRADOS DE MADUREZ DE PROCESOS - SEGUROS DEL PICHINCHA			
PROCESOS DE TI – COBIT		Grado de Madurez	Nivel de Madurez
Evaluar, Orientar y Supervisar			**3***
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno	66,67%	4
EDM02	Asegurar la entrega de beneficios	77,78%	4
EDM03	Asegurar la optimización del riesgo	60,00%	3
EDM04	Asegurar la optimización de los recursos	50,00%	3
EDM05	Asegurar la transparencia hacia las partes interesadas	60%	3
Alinear, Planificar y Organizar			**3***
APO01	Gestionar el marco de gestión de TI	66,67%	4
APO02	Gestionar la estrategia	77,78%	4
APO03	Gestionar la arquitectura empresarial	80,00%	4
APO04	Gestionar la innovación	87,50%	3
APO05	Gestionar portafolio	83,33%	3
APO06	Gestionar el presupuesto y los costes	50,00%	3
APO07	Gestionar los recursos humanos	60,00%	3
APO08	Gestionar las relaciones	60,00%	3
APO09	Gestionar los acuerdos de servicio	50,00%	3
APO10	Gestionar los proveedores	60,00%	3
APO11	Gestionar la calidad	66,67%	2
APO12	Gestionar el riesgo	77,78%	4
AP013	Gestionar la seguridad	77,78%	4
Construcción, Adquisición e Implementación			**3***
BAI01	Gestionar los programas y proyectos	100,00%	4
BAI02	Gestionar la definición de requisitos	80,00%	3
BAI03	Gestionar la identificación y la construcción de soluciones	100,00%	5
BAI04	Gestionar la disponibilidad y la capacidad	50,00%	3
BAI05	Gestionar la introducción de cambios organizativos	100,00%	3
BAI06	Gestionar los cambios	55,56%	4
BAI07	Gestionar la aceptación del cambio y de la transición	62,50%	4
BAI08	Gestionar el conocimiento	50,00%	3
BAI09	Gestionar los activos	100,00%	4
BAI10	Gestionar la configuración	80,00%	3
Entregar, dar Servicio y Soporte			**4***
DSS01	Gestionar las operaciones	75,00%	4
DSS02	Gestionar las peticiones y los incidentes del servicio	71,43%	4
DSS03	Gestionar los problemas	50%	3
DSS04	Gestionar la continuidad	75,00%	4
DSS05	Gestionar los servicios de seguridad	60,00%	4
DSS06	Gestionar los controles de los procesos del negocio	57,14%	4
Supervisión, Evaluación y Verificación			**3***
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad	87,50%	3
MEA02	Supervisar, evaluar y valorar el sistema de control interno	57,14%	3
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos	45,45%	5

***Los valores son obtenidos de la moda de los procesos correspondientes

Tabla A5.7. Matriz de Grados de Procesos – Seguros del Pichincha (COBIT 5, 2012)

MATRIZ DE NIVEL DE SERVICIO - SEGUROS DEL PICHINCHA									
		DESEMPEÑO							
PROCESOS DE TI – COBIT		NO CUMPLE	CUMPLE LEVEMENTE	CUMPLE PARCIALMENTE	CUMPLE MAYORITARIAMENTE	CUMPLE CASI TOTALMENTE	CUMPLE TOTALMENTE	%	
Evaluar, Orientar y Supervisar: Gobierno asegura que los objetivos de la empresa se logren mediante la evaluación de las necesidades de las partes interesadas teniendo en cuenta las condiciones y opciones, estableciendo la dirección a través de la priorización y decisión, monitoreando el desempeño, el cumplimiento y el progreso comparando con la dirección y objetivos								**62,93%**	
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno						X	92,89%	
EDM02	Asegurar la entrega de beneficios			X				56,69%	
EDM03	Asegurar la optimización del riesgo				X			62,96%	
EDM04	Asegurar la optimización de los recursos				X			62,96%	
EDM05	Asegurar la transparencia hacia las partes interesadas		X					39,17%	
Alinear, Planificar y Organizar: Cubre el uso de la información y la tecnología y como esta puede ser usada para lograr los objetivos y las metas de la compañía.								**63,32%**	
APO01	Gestionar el marco de gestión de TI					X		67,78%	
APO02	Gestionar la estrategia				X			61,11%	
APO03	Gestionar la arquitectura empresarial				X			67,33%	
APO04	Gestionar la innovación					X		75,83%	
APO05	Gestionar portafolio			X				50,67%	
APO06	Gestionar el presupuesto y los costes			X				54,17%	
APO07	Gestionar los recursos humanos					X		67,78%	
APO08	Gestionar las relaciones					X		67,33%	
APO09	Gestionar los acuerdos de servicio					X		71,48%	
APO10	Gestionar los proveedores			X				54,07%	
APO11	Gestionar la calidad		X					45,19%	
APO12	Gestionar el riesgo					X		74,67%	
AP013	Gestionar la seguridad				X			65,71%	
Construcción, Adquisición e Implementación: Cubre la identificación de requerimientos de TI, adquiere la tecnología y la implementa dentro de los procesos de negocio actuales de la compañía								**58,59%**	
BAI01	Gestionar los programas y proyectos				X			62,96%	
BAI02	Gestionar la definición de requisitos		X					39,17%	
BAI03	Gestionar la identificación y la construcción de soluciones			X				48,00%	
BAI04	Gestionar la disponibilidad y la capacidad			X				44,81%	
BAI05	Gestionar la introducción de cambios organizativos					X		75,00%	
BAI06	Gestionar los cambios					X		75,19%	
BAI07	Gestionar la aceptación del cambio y de la transición					X		75,19%	
BAI08	Gestionar el conocimiento				X			60,00%	
BAI09	Gestionar los activos			X				48,89%	
BAI10	Gestionar la configuración			X				56,67%	
Entregar, dar Servicio y Soporte: Entrega, Soporte y Servicio., Asegura la continuidad de la operación desde la gestión y atención de incidentes y problemas mitigando los riesgos y aportando la seguridad necesaria para que las funciones importantes de soporte de TI se realicen regularmente y en forma debida								**57,14%**	
DSS01	Gestionar las operaciones			X				48,33%	
DSS02	Gestionar las peticiones y los incidentes del servicio			X				50,83%	
DSS03	Gestionar los problemas				X			61,85%	
DSS04	Gestionar la continuidad				X			69,26%	
DSS05	Gestionar los servicios de seguridad				X			69,63%	
DSS06	Gestionar los controles de los procesos del negocio			X				42,96%	
Supervisión, Evaluación y Verificación: Evalúa las necesidades de la empresa si el actual sistema de TI cumple con los objetivos para los cuales fue diseñado y si están establecidos los controles necesarios para cumplir con los requerimientos regulatorios.								**64,22%**	
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad			X				57,50%	
MEA02	Supervisar, evaluar y valorar el sistema de control interno				X			64,44%	
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos					X		70,74%	

Tabla A5.8. Matriz de Nivel de usuarios – Seguros del Pichincha (COBIT 5, 2012)

MATRIZ DE IMPACTO DE PROCESOS FRENTE A LOS CRITERIOS DE INFORMACIÓN DE COBIT															
		CRITERIOS DE INFORMACION DE COBIT							R ECURSOS DE TI				IMPACTO
PROCESOS DE TI - COBIT		UTILIDAD	USABILIDAD	CREDIBILIDAD	LIBRE DE ERROR	ACCESIBILIDAD	SEGURIDAD	CONFORMIDAD	PERSONAS	INFORMACIÓN	APLICACIÓN	INFRAESTRUCTURA	%
Evaluar,Orientar y Supervisar													**77,93%**
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno	0,86	0,63				0,32		X	X	X	X	75,00%
EDM02	Asegurar la entrega de beneficios	0,63	0,86	0,63	0,86			0,32	X	X		X	56,69%
EDM03	Asegurar la optimización del riesgo	0,86				0,86		0,63	X	X	X	X	86,00%
EDM04	Asegurar la optimización de los recursos	0,86	0,86				0,32		X	X	X	X	86,00%
EDM05	Asegurar la transparencia hacia las partes interesadas	0,86	0,86						X			X	86,00%
Alinear, Planificar y Organizar													**66,46%**
APO01	Gestionar el marco de gestión de TI	0,86	0,86	0,63	0,63	0,63	0,63	0,63	X	X	X	X	86,00%
APO02	Gestionar la estrategia	0,86	0,86	0,63	0,63	0,63	0,63	0,63	X	X	X	X	86,00%
APO03	Gestionar la arquitectura empresarial	0,86	0,86			0,63					X	X	86,00%
APO04	Gestionar la innovación	0,86	0,63			0,86			X	X	X	X	75,00%
APO05	Gestionar portafolio		0,32	0,86	0,86	0,63	0,63	0,63	X	X	X	X	16,00%
APO06	Gestionar el presupuesto y los costes		0,86					0,86	X	X	X	X	43,00%
APO07	Gestionar los recursos humanos	0,86	0,63			0,32			X				75,00%
APO08	Gestionar las relaciones	0,86	0,86			0,32			X		X		86,00%
APO09	Gestionar los acuerdos de servicio	0,86	0,63			0,63		0,63		X	X	X	75,00%
APO10	Gestionar los proveedores	0,86	0,86			0,63			X	X	X	X	86,00%
APO11	Gestionar la calidad	0,32	0,32		0,86			0,86		X			32,00%
APO12	Gestionar el riesgo	0,32	0,32		0,86	0,86						X	32,00%
AP013	Gestionar la seguridad	0,86	0,86		0,63	0,63			X	X	X	X	86,00%
Construcción, Adquisición e Implementación													**77,20%**
BAI01	Gestionar los programas y proyectos	0,86	0,63				0,32		X	X	X	X	75,00%
BAI02	Gestionar la definición de requisitos	0,63	0,86	0,63	0,86					X	X		75,00%
BAI03	Gestionar la identificación y la construcción de soluciones	0,86	0,86					0,32			X	X	86,00%
BAI04	Gestionar la disponibilidad y la capacidad	0,86	0,86						X				86,00%
BAI05	Gestionar la introducción de cambios organizativos	0,86	0,86		0,32			0,63	X		X	X	86,00%
BAI06	Gestionar los cambios	0,86					0,63		X	X			43,00%
BAI07	Gestionar la aceptación del cambio y de la transición	0,86	0,86						X				86,00%
BAI08	Gestionar el conocimiento	0,86	0,86		0,63			0,63	X	X	X	X	86,00%
BAI09	Gestionar los activos	0,63	0,63	0,86	0,86	0,86	0,63	0,63	X	X	X	X	63,00%
BAI10	Gestionar la configuración	0,86	0,86						X		X	X	86,00%
Entregar, dar Servicio y Soporte													**80,50%**
DSS01	Gestionar las operaciones	0,86	0,63				0,32				X	X	75,00%
DSS02	Gestionar las peticiones y los incidentes del servicio	0,86	0,86		0,63			0,63			X		86,00%
DSS03	Gestionar los problemas		0,86		0,63	0,63						X	75,00%
DSS04	Gestionar la continuidad	0,86	0,86		0,63	0,63	0,63	0,63	X		X	X	86,00%
DSS05	Gestionar los servicios de seguridad	0,63	0,86				0,63		X	X	X	X	75,00%
DSS06	Gestionar los controles de los procesos del negocio	0,86	0,86		0,86	0,86		0,63	X	X	X	X	86,00%
Supervisión, Evaluación y Verificación													**86,00%**
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad	0,86	0,86	0,63	0,63	0,63	0,63	0,63	X	X	X	X	86,00%
MEA02	Supervisar, evaluar y valorar el sistema de control interno	0,86	0,86	0,63	0,63	0,63	0,63	0,63	X	X	X	X	86,00%
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos	0,86	0,86				0,86	0,63	X	X	X	X	86,00%

Tabla A5.9. Matriz de Cumplimiento de Objetivos de Gobierno (COBIT 5,2012)

MATRIZ DE DIAGNOSTICO DE PROCESOS COBIT																
		IMPORTANCIA				FORMALIZADO/ NORMADO				CONTROL INTERNO			AUDITADO		
PROCESOS DE TI – COBIT		POCO IMPORTANTE	IMPORTANTE	MUY IMPORTANTE	%	NO FORMALIZADO	FORMALIZADO	NO APLICA	NO SE SABE CON CERTEZA	NO DOCUMENTADO	DOCUMENTADO	NO SE SABE CON CERTEZA	NO AUDITADO	AUDITADO	NO SE SABE CON CERTEZA
Evaluar,Orientar y Supervisar					**100,00%**										
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno			X	100,00%	x				X			X		
EDM02	Asegurar la entrega de beneficios			X	100,00%	x				X			X		
EDM03	Asegurar la optimización del riesgo			X	100,00%		x				X		X		
EDM04	Asegurar la optimización de los recursos		X		67,00%		x				X		X		
EDM05	Asegurar la transparencia hacia las partes interesadas	X			33,00%	x				X			X		
Alinear, Planificar y Organizar					**53,85%**										
APO01	Gestionar el marco de gestión de TI		X		67,00%		x				x		x		
APO02	Gestionar la estrategia	X			33,00%		x				x		x		
APO03	Gestionar la arquitectura empresarial	X			33,00%	x				x			x		
APO04	Gestionar la innovación			X	100,00%		x				x		x		
APO05	Gestionar portafolio		X		67,00%	x					x		x		
APO06	Gestionar el presupuesto y los costes		X		67,00%		x				x		x		
APO07	Gestionar los recursos humanos	X			33,00%	x				x			x		
APO08	Gestionar las relaciones	X			33,00%		x				x		x		
APO09	Gestionar los acuerdos de servicio		X		67,00%		x			x			x		
APO10	Gestionar los proveedores	X			33,00%		x			x			x		
APO11	Gestionar la calidad		X		67,00%	x					x		x		
APO12	Gestionar el riesgo	X			33,00%		x				x		x		
AP013	Gestionar la seguridad		X		67,00%	x				x			x		
Construcción, Adquisición e Implementación					**70,10%**										
BAI01	Gestionar los programas y proyectos			X	100,00%	X				X			X		
BAI02	Gestionar la definición de requisitos			X	100,00%	X				X			X		
BAI03	Gestionar la identificación y la construcción de soluciones			X	100,00%		X				X		X		
BAI04	Gestionar la disponibilidad y la capacidad		X		67,00%		X				X		X		
BAI05	Gestionar la introducción de cambios organizativos	X			33,00%	X				X			X		
BAI06	Gestionar los cambios		X		67,00%		X				X		X		
BAI07	Gestionar la aceptación del cambio y de la transición		X		67,00%		X				X		X		
BAI08	Gestionar el conocimiento	X			33,00%	X				X			X		
BAI09	Gestionar los activos		X		67,00%		X				X		X		
BAI10	Gestionar la configuración		X		67,00%	X					X		X		
Entregar, dar Servicio y Soporte					**77,83%**										
DSS01	Gestionar las operaciones			X	100,00%	X				X			X		
DSS02	Gestionar las peticiones y los incidentes del servicio			X	100,00%		X				X		X		
DSS03	Gestionar los problemas		X		67,00%		X				X		X		
DSS04	Gestionar la continuidad	X			33,00%		X				X				
DSS05	Gestionar los servicios de seguridad			X	100,00%		X				X			X	
DSS06	Gestionar los controles de los procesos del negocio		X		67,00%		X				X		X		
Supervisión, Evaluación y Verificación					**66,67%**										
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad		X		67,00%	X					X		X		
MEA02	Supervisar, evaluar y valorar el sistema de control interno	X			33,00%	X				X			X		
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos			X	100,00%		X				X		X		

Tabla A5.10. Matriz de Impacto de Procesos frente a los criterios de Información de COBIT (COBIT 5,2012)